FortiAuthenticator™

Interoperability Guide

FortiAuthenticator™ Interoperability Guide

June 27, 2014

Revision 8

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2013-10-11	Initial revision
2	2012-04-03	Update to FortiAuthenticator 1.0 MR3. Added FortiMail, FortiWeb, Citrix Access Gateway
3	2012-06-20	Update to include challenge-response authentication method for FortiGate and Cisco IOS
4	2012-09-21	Update to add Cisco IOS
5	2012-11-01	Update document template
6	2012-12-05	Add F5 Big-IP Configuration
7	2013-10-24	Update for FortiAuthenticator 3.0
8	2014-06-26	Update for FortiAuthenticator 3.1

Introduction

This document has been produced to aid the configuration of the FortiAuthenticator Secure Authentication system with Fortinet solutions and other third party products.

Software versions

Testing was performed with the following versions of software where applicable:

- FortiAuthenticator 3.1 GA
- FortiGate 5.0 PR7 & 5.2
- FortiWeb
- FortiClient 5.0.9
- FortiManager 5.0 PR6
- FortiAuthenticator 5.0 PR6
- FortiMail 5.1.x
- Ubuntu 11.04
- OpenSSH version 5.8p1
- Apache version 2.2.17
- Citrix Access Gateway 5.0

Basic Configuration of the FortiAuthenticator

The Basic configuration of the FortiAuthenticator is shown below. Any deviations or change which are required from this configuration will be detailed in the relevant section.

For more detail on the setup and configuration of the FortiAuthenticator see the Administration Guide at http://docs.fortinet.com/fortiauthenticator/admin-guides.

Basic Configuration

On first boot, the FortiAuthenticator is configured to the default settings:

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

These setting can be modified by configuring a PC to an address on the same subnet and accessing the Web GUI via https://192.168.1.99/, alternatively you can use the CLI method below.

Configuration Using the CLI

Basic configuration of the interface IP and gateway address can be done using the Command Line Interface (CLI).

Connect the Management Computer to the FortiAuthenticator unit using the supplied Console Cable

Using a suitable terminal emulation program connect to the unit with the following settings:

```
Baud Rate: 9600
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None
```

Log in to the FortiAuthenticator unit using the default credentials below:

```
Username: admin
Password: <blank>
```

Configure the network settings as required, for example:

```
set port1-ip 10.1.1.99/24
set default-gw 10.1.1.1
```

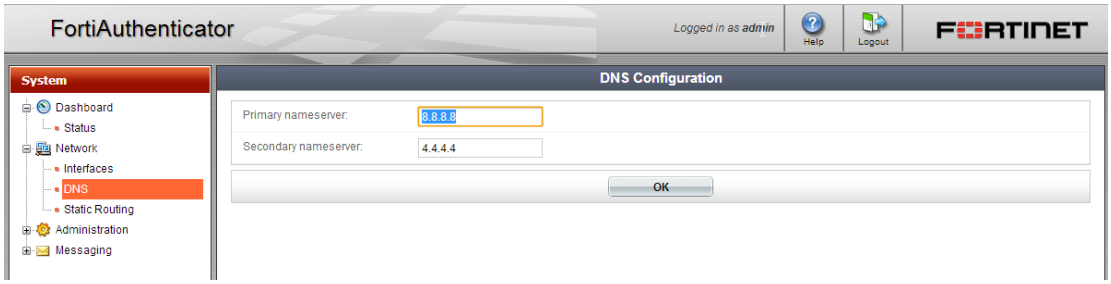
This will give you access to the GUI via the specified IP address, in this case https://10.1.1.99

System Settings

Once the basic networking has been configured, further configuration can be performed via the GUI.

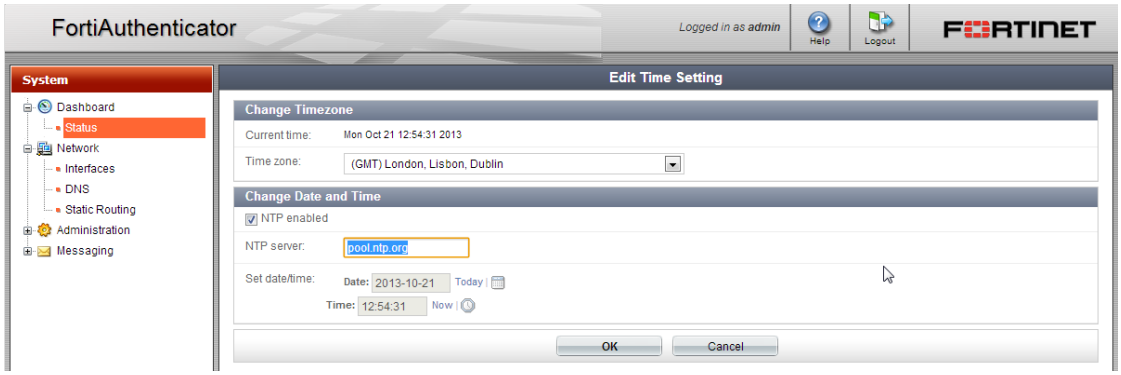
DNS

To enable resolution of the FortiGuard network and other systems such as NTP servers, set your DNS to your local or ISP nameserver configuration via *System → Network → DNS*.



Time Synchronization

FortiToken two-factor authentication uses a time based algorithm to generate Token PINs for use in the authentication process. It is therefore essential that the time is accurate on the FortiAuthenticator system and NTP time synchronization is recommended. Change your settings to a local NTP server for accurate timing via *Dashboard → Status → System Time and click **[Change]***.

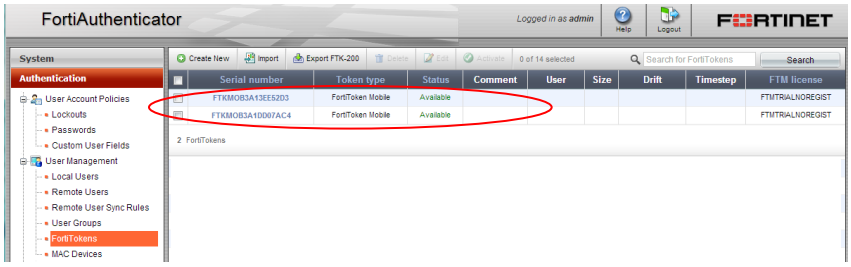


Create a test token

For testing two-factor authentication, a FortiToken will be required.

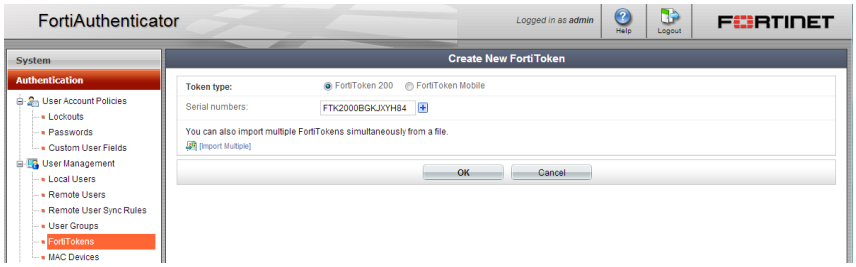
FortiToken Mobile

By default, each new installation comes with 2 FortiToken Mobile Tokens included which can be used free of charge for testing purposes

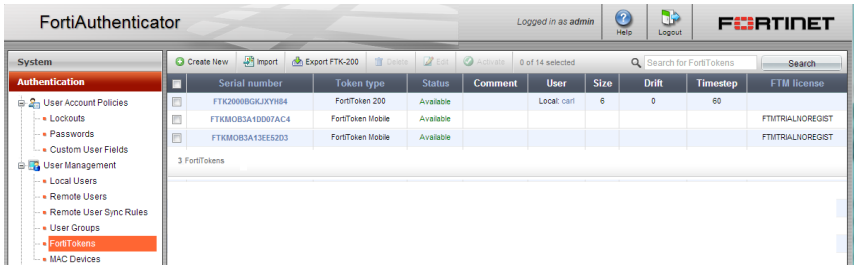


FortiToken 200 (TOTP)

To register a new physical token (FTK200) go to *Authentication → User Management → FortiTokens* and select ***Create New***. For single tokens, enter the token serial in the Serial Numbers dialogue box. To register multiple tokens, select the 

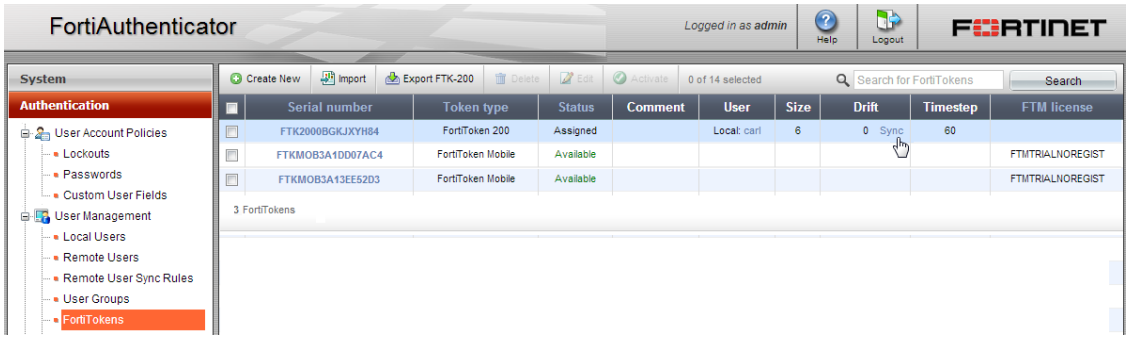


Once registered the token should show as status ***Available*** in the *Authentication → User Management → FortiTokens* page.



Synchronizing Tokens

When new, all tokens are set to a drift of 0 which is a measure of how close the time on the token and time on the FortiAuthenticator match. When new, this should be 0. If you are unable to authenticate at any time, this may be due to clock drift. To force a token drift synchronization, hover the mouse over the drift section for the token and click the ***Sync*** option which is displayed.



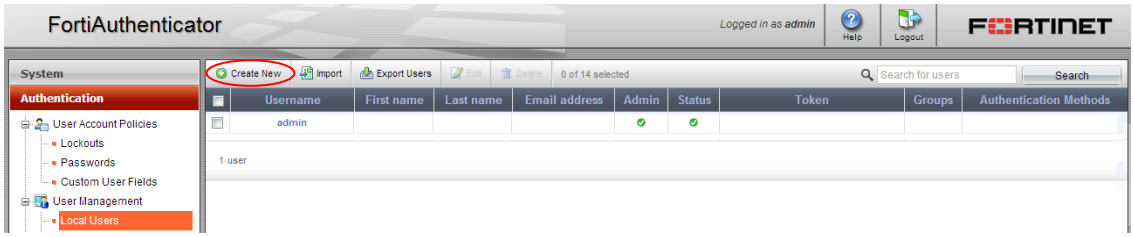
You will be prompted to enter 2 consecutive PINs from the token. Ensure you have not just used the number for an authentication attempt; if so, wait until the next number refreshed. Once synchronized wait until the next refresh before attempting to authenticate (token PINs are for one-time use, regardless of what they are used for).

Create test users

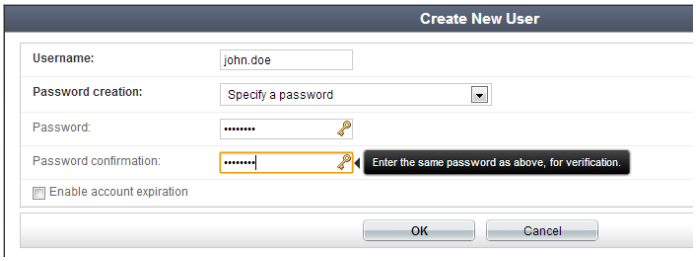
For the purpose of this interoperability test, a single user will be created:

`john.doe`	Test user with RADIUS based username / password and FortiToken configured. Member of the RADIUS_Admins group.
`jane.doe`	Test user with RADIUS based username / password and FortiToken configured. Member of the RADIUS_Viewers group.
`restricted.user`	Test user with no RADIUS token and not a member of any group.

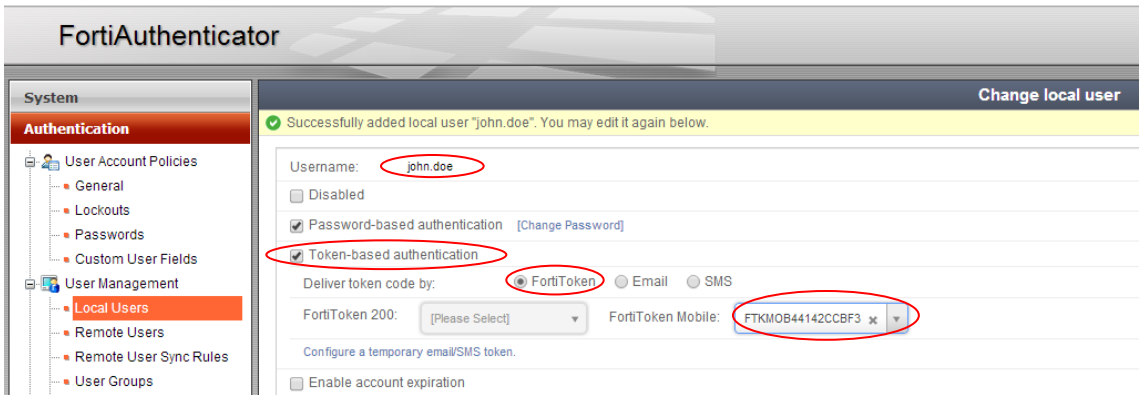
In *Authentication → User Management → Local Users* select ***Create New***



In the resulting dialogue, enter a username and password for this test user account



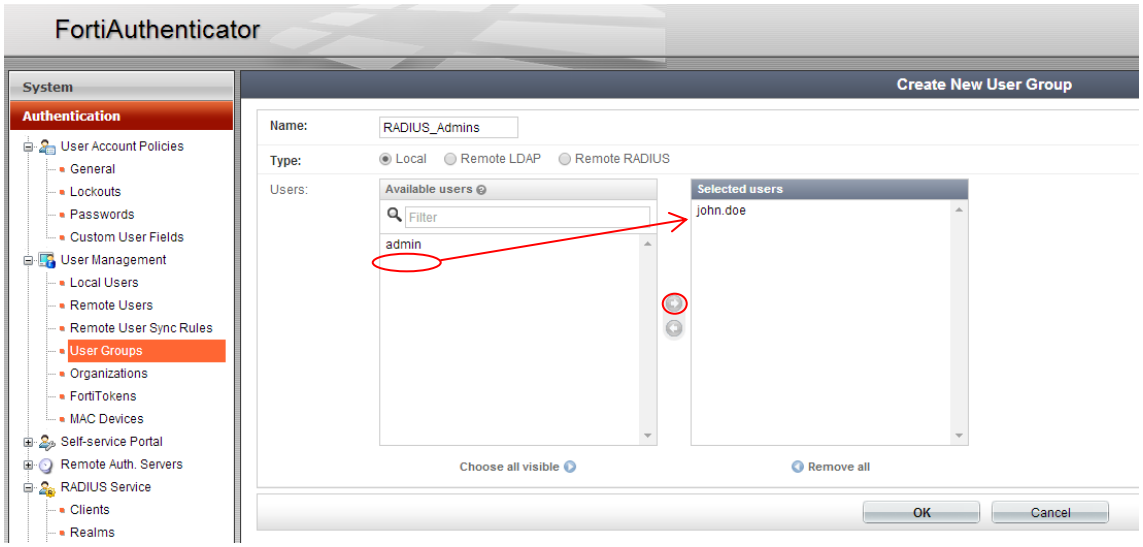
Once created, you will be provided with additional options to edit for the user. For the purpose of this document, all that is needed is to *enable Two-factor authentication* by ticking the radio buttons and select the token serial you have just created from the drop down menu.



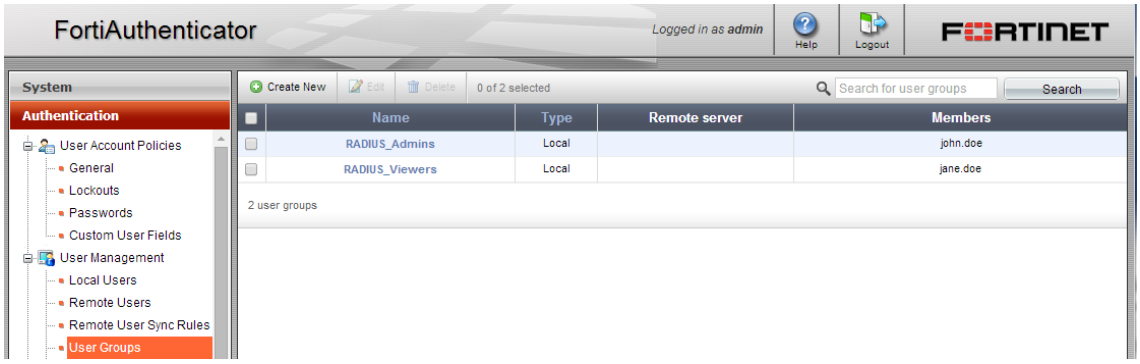
Repeat the process to create an additional user called “restricted.user” and do not make this user a member of any group. This user will be used throughout the testing to prove that only members of the specified groups have permission to authenticate.

Create User Groups

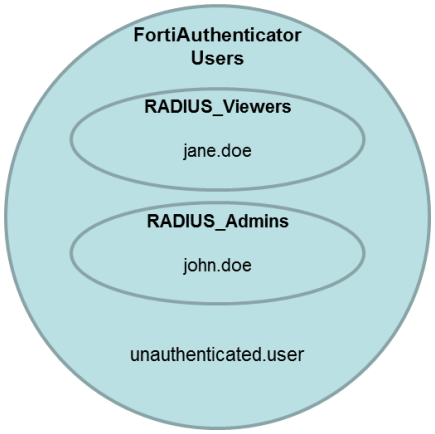
On FortiAuthenticator, in *User → User Group*, select *Create New*. ***Create*** a group called *RADIUS_Admins*, selecting the test user john.doe and the right arrow to make them part of the group.



Repeat the process to ***Create*** a group called *RADIUS_Viewers*, selecting the test user jane.doe and the right arrow to make them part of the group.

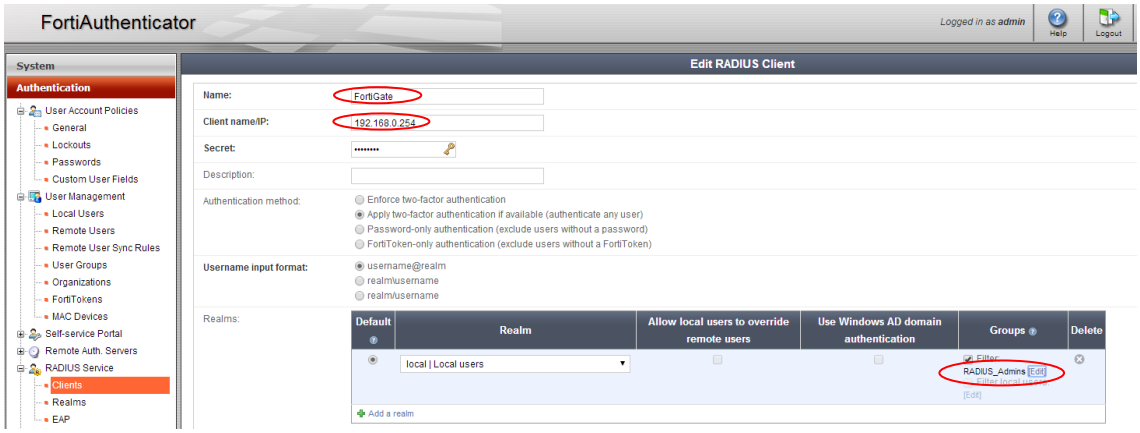


Once completed, the users/groups membership should appear like the following



Configure a RADIUS Client

Before any device can connect to the FortiAuthenticator to authenticate users via RADIUS, it must be configured as a RADIUS Client. For security reasons, until this is done, the FortiAuthenticator will ignore all authentication requests. In *Authentication → RADIUS Service → Clients,* select ***Create New*** and on the resulting page, enter the details of the device you wish to authenticate.



- Enter a unique name for the device and the IP from which it will be connecting. Note that this is the IP address of the device itself, not the IP that the users will be authenticating from.
- In the secret section, enter a secret password which will be used by both ends of the RADIUS connection to secure the authentication process.
- Select “Apply Two-Factor authentication if available”. This will allow bother users with and without tokens to authenticate for the purpose of testing.
- Select Local users to be authenticated at this point

You will have to repeat this process for every device you wish to authenticate against the FortiAuthenticator.

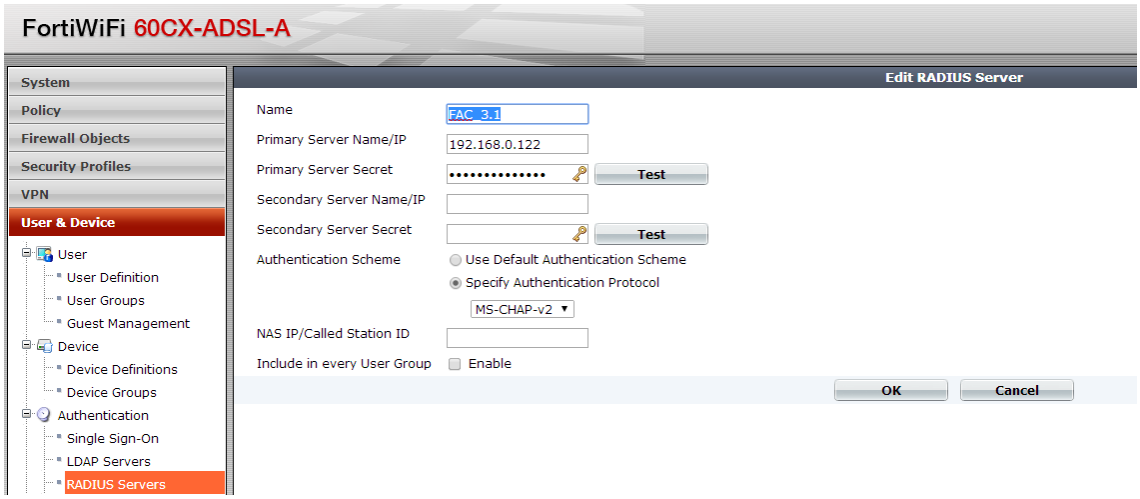
FortiGate (Admin Users)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration". Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The FortiGate appliance is the Gateway to your network therefore securing remote access, whether to the box itself (administration) or to the network behind it (VPN) is critical. FortiOS versions 4.0 MR3 and above natively support two-factor authentication using FortiToken, however to perform two factor authentication to multiple FortiGate devices with a single FortiToken or lower versions, a FortiAuthenticator is required.

Create Remote RADIUS Connection

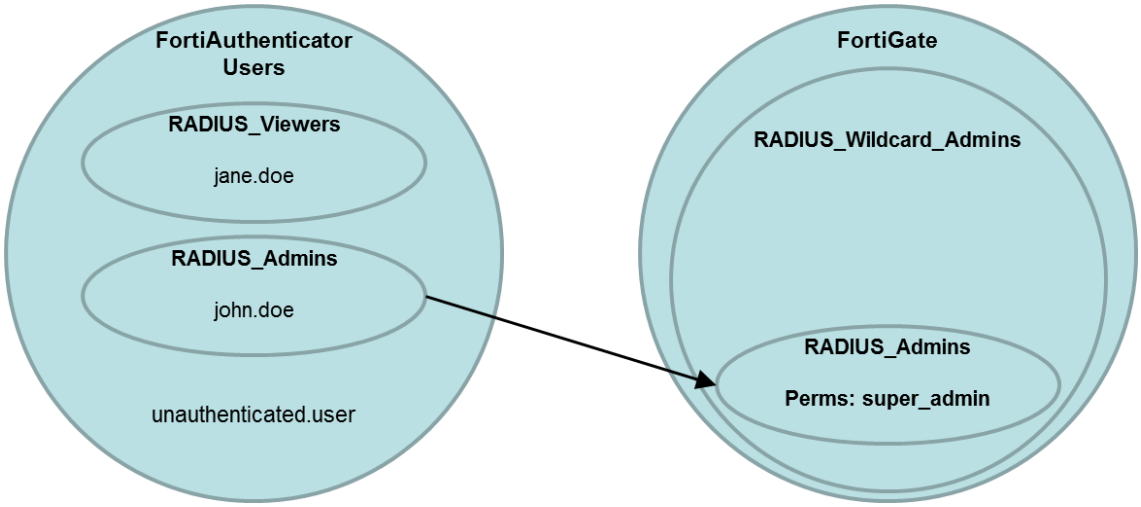
A RADIUS association is required for all FortiGate configurations described below so configure the system to point at the FortiAuthenticator. In *User → Remote → RADIUS* select ***Create New*** and configure the details of the FortiAuthenticator. Enter the shared secret which you created previously.



In *User & Device → User → User Groups* select ***Create New*** and configure a new Firewall group called RADIUS_Users, adding the FortiAuthenticator RADIUS server created above (FAC_3.1) as a member.

Single Group Defined Admin Users

When the RADIUS Client (NAS) was defined on the FortiAuthenticator in the section titled Create User Groups, the FortiAuthenticator was configured to authenticate the group "RADIUS_Admins". In this example we will use this to map all such users to the Super_Admin permission. No other users will be authenticated.

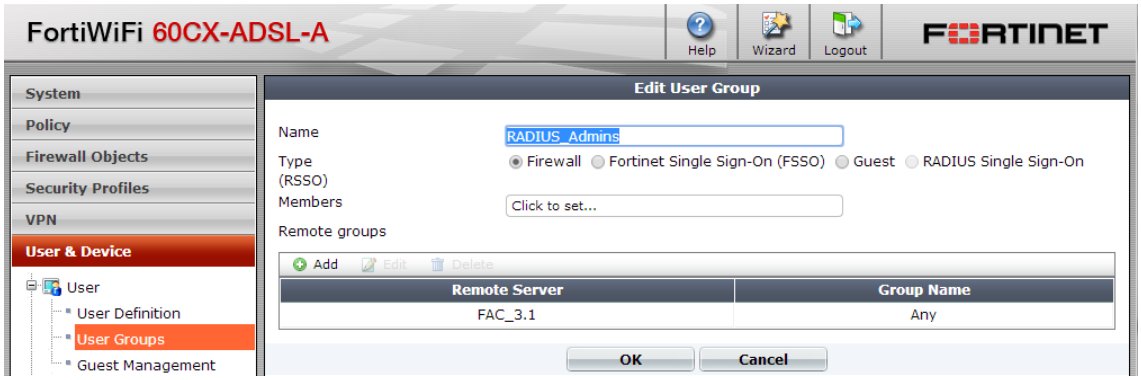


Create RADIUS_Admins user group on FortiGate

In User & Device → User → User Groups, select *Create New*. Create a user group of Type Firewall with name RADIUS_Admins.

Select Add, to attach a Remote Server to the Group and select your FortiAuthenticator.

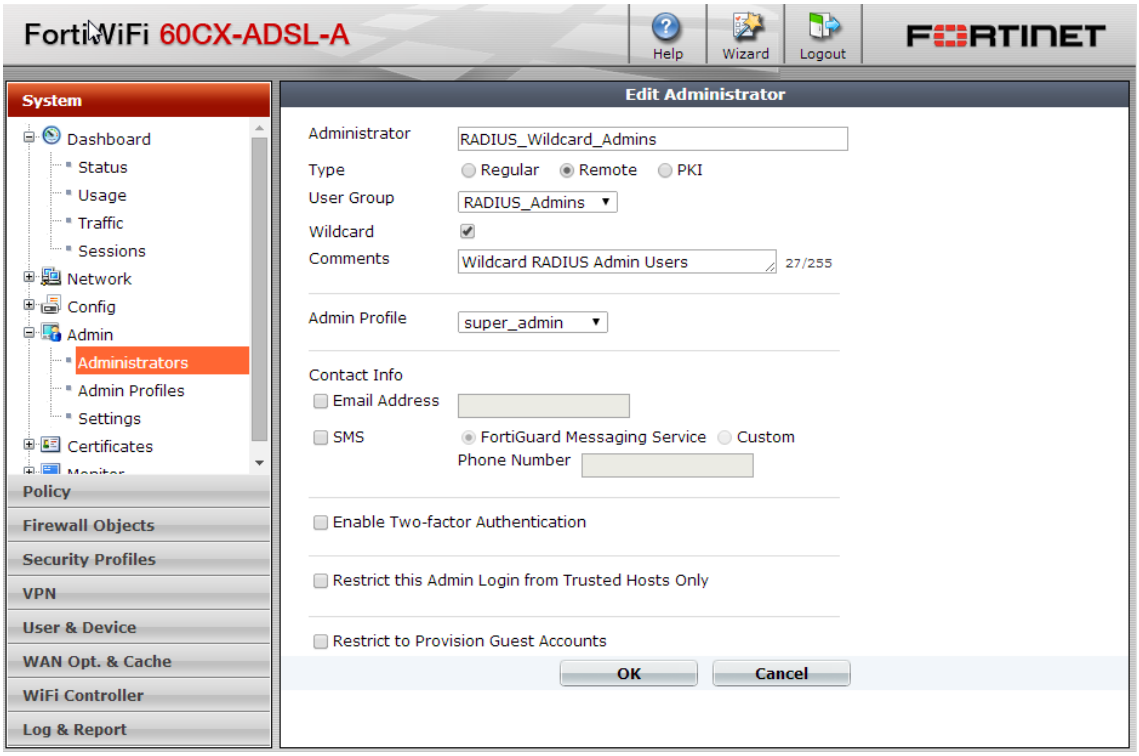
For this example, select Group Name "Any". This is because the FortiAuthenticator was configured in the previous step to only authenticate users from the group "RADIUS_Admins".



Create Wildcard Admin User

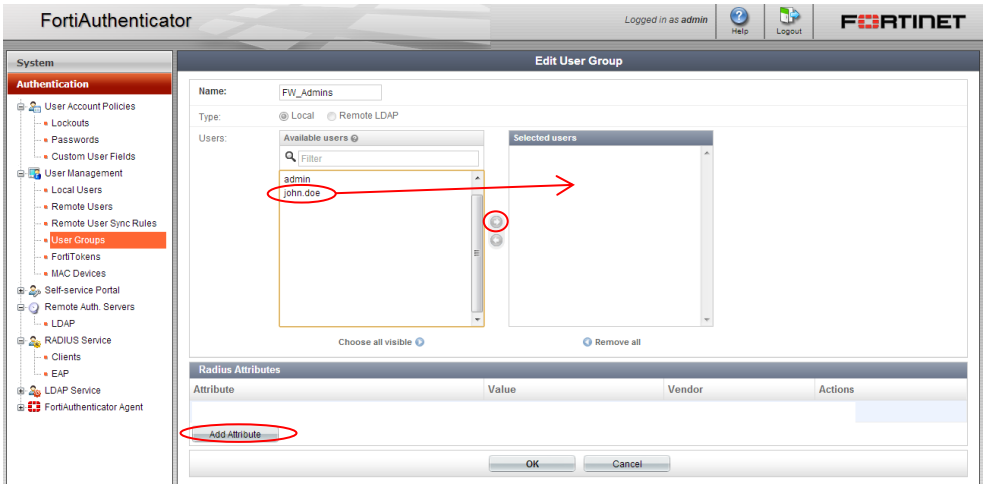
In *System → Admin → Administrators*, select *Create New*. In the resulting page, enter

Administrator:	**RADIUS_Wildcard_Admins**
Type:	**Remote**
User Group:	**RADIUS_Admins**
Wildcard:	**<ticked>**
Admin Profile:	**super_admin**



Caution:

Do not select two-factor authentication at this point. The Two Factor Authentication is done externally on the FortiAuthenticator, so the FortiGate does not need any configuration. This is why the FortiAuthenticator is capable of providing two-factor authentication to FortiOS 4.2 and below and third party systems which have no direct support for two-factor authentication.



Testing

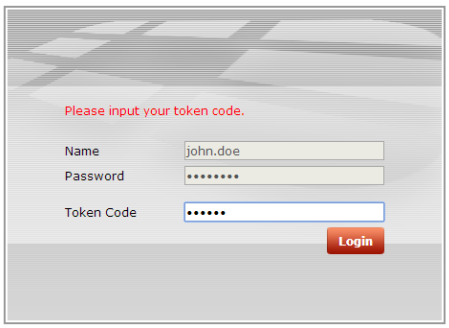
Attempt to log into the FortiGate Administration GUI using the john.doe credentials

`Username:` ***`john.doe`***

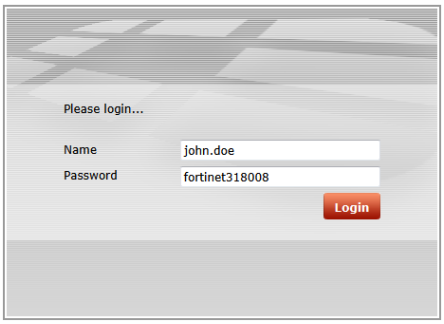
Password: **<password>**

Token: **<Token Passcode>**

e.g.



It is also possible to authenticate using a concatenated passcode e.g. for a Password “fortinet” and one-time PIN of 318008, the login would become



However, obviously the password would be starred out.

Login via the will also be protected similarly e.g.

```
login as: john.doe
john.doe@192.168.0.254's password:
Remote Token:******
FortiGate01 #
```

Successful authentication will provide the user with access to the device and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
175	Fri Aug 19 14:12:51 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

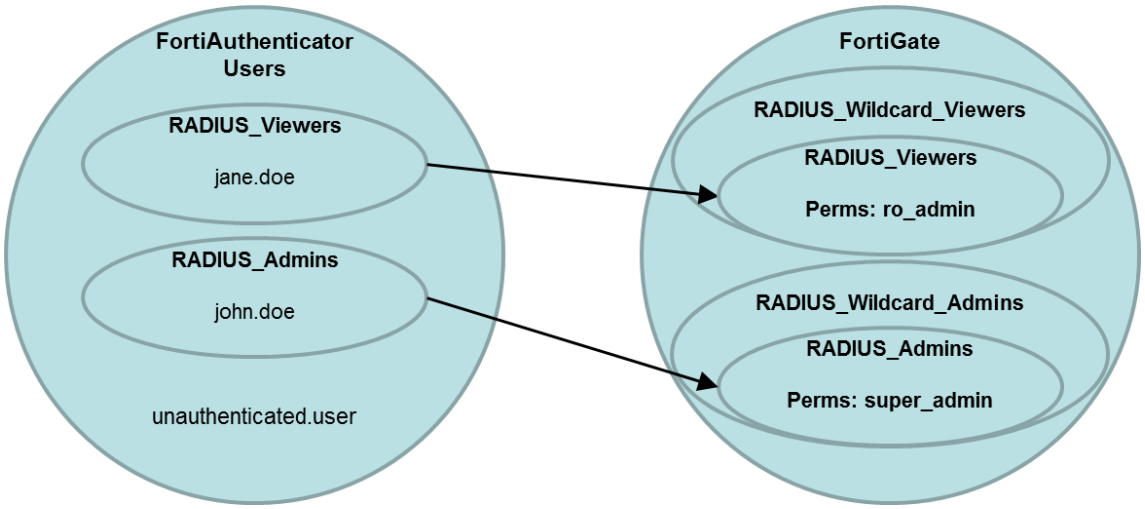
If authentication is unsuccessful, follow the steps in the Chapter **Appendix** A – Debugging to identify what is wrong.

Results

User	Permission granted
john.doe	super_admin
jane.doe	Login failed
Unauthenticated.user	Login failed

Multiple Group Defined Admin Users

There are many situations where multiple administrative user groups are required on the FortiGate. These could include situations where support have access to view the configuration, or where there are users with limited admin rights. This section will demonstrate how this can be achieved to deliver the multiple administrative permission levels.

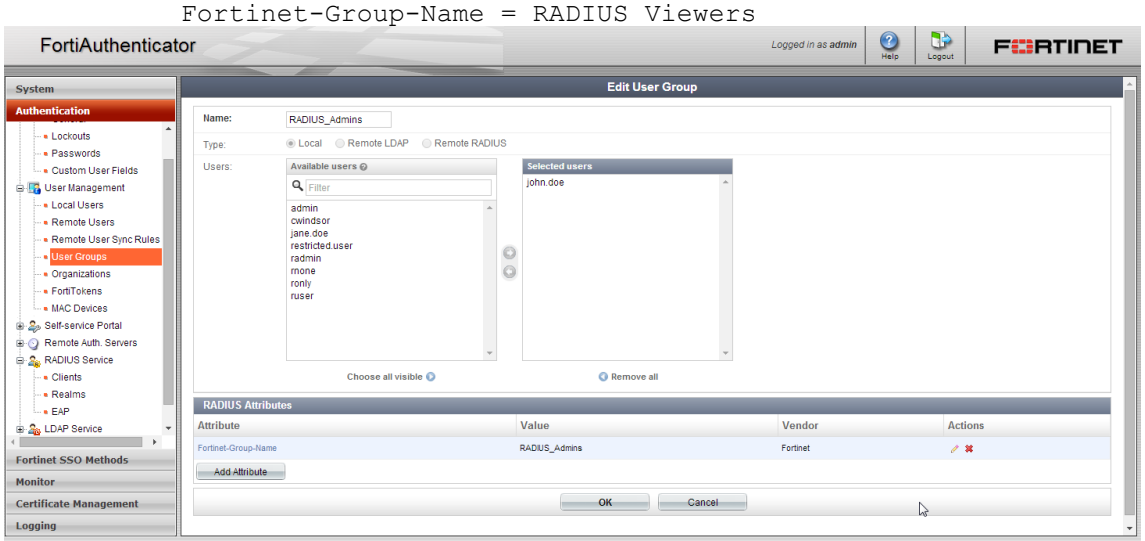


Modify FortiAuthenticator Groups

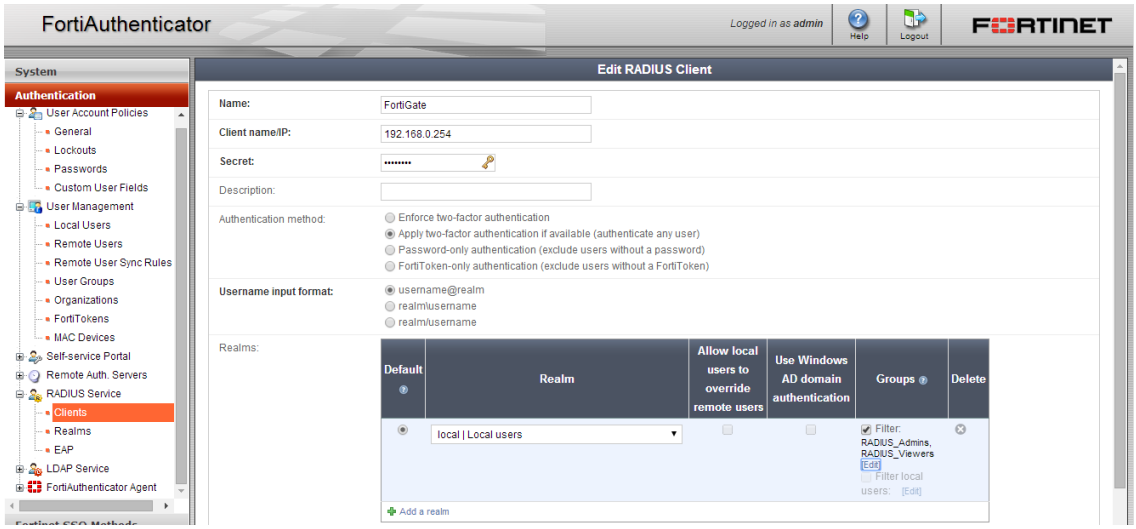
When multiple groups are configured FortiGate needs to differentiate users based on their FortiAuthenticator group membership. To do this, FortiAuthenticator must be configured to send group information with the RADIUS Access-Accept packet.

To do this, configure the RADIUS Attribute Fortinet-Group-Name for each Group as shown below.

```
Name: RADIUS_Admins
      Fortinet-Group-Name = RADIUS_Admins
Name: RADIUS_Viewers
      Fortinet-Group-Name = RADIUS Viewers
```



Once the two groups have been created, they must be added to the group list authenticated for that RADIUS Client / NAS as shown.

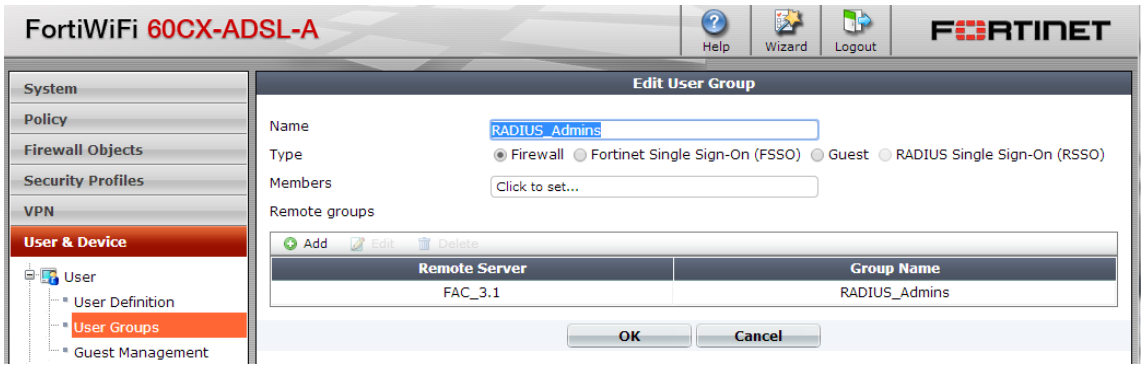


Create user groups on FortiGate

In *User & Device → User → User Groups*, select ***Create New***. Create 2 user groups of *Type Firewall* with *Name* RADIUS_Admins & RADIUS_Viewers.

Select ***Add***, to attach a Remote Server to the Group and select your FortiAuthenticator.

In this example, FortiAuthenticator will be authenticating multiple groups so we will need to differentiate between them. Select Group Name and enter the appropriate group for each e.g.



Create Wildcard Admin Users

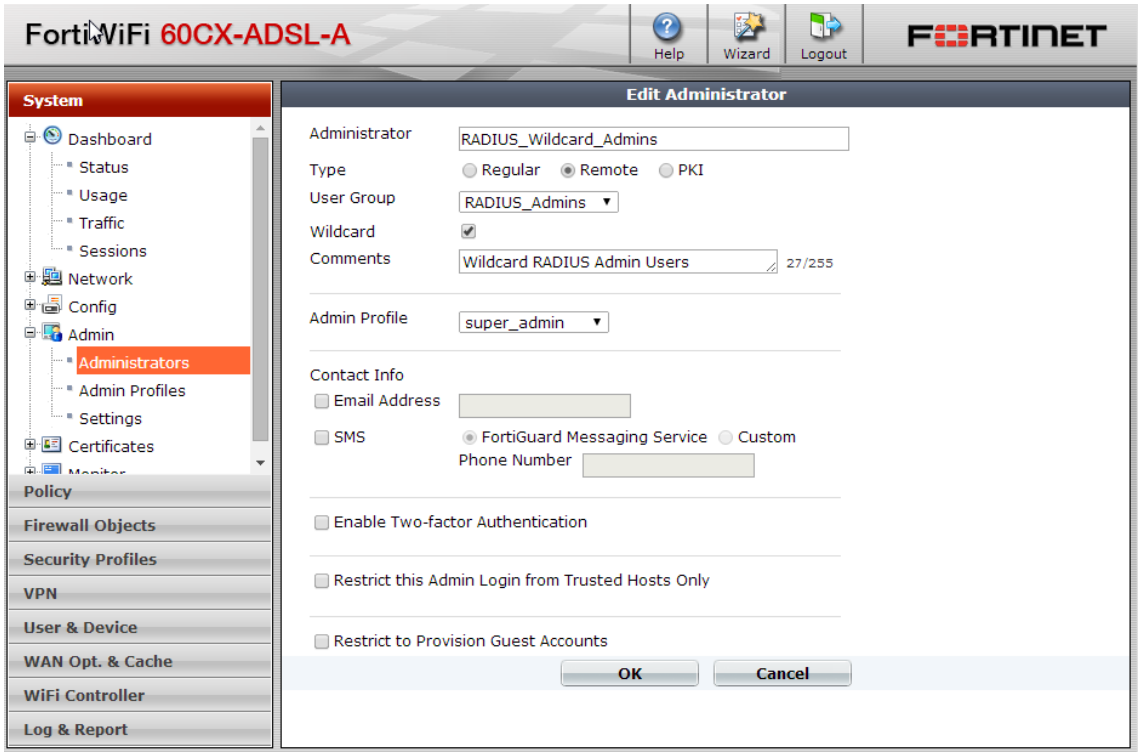
You will need to map the RADIUS Groups to the Admin Permissions. To achieve this, create 2 new wildcard admin users. In *System → Admin → Administrators*, select ***Create New***. In the resulting page, create a new user:

```
Administrator:          RADIUS_Wildcard_Admins
Type:                   Remote
User Group:             RADIUS_Admins
Wildcard:               <ticked>
Admin Profile:          super_admin
```

Repeat this process, for the RADIUS_Viewers account

```
Administrator:          RADIUS_Wildcard_Viewers
Type:                   Remote
User Group:             RADIUS_Viewers
Wildcard:                       <ticked>
Admin Profile:                  ro_admin
```

Where ro_admin is an admin profile allowing only read only access to the configuration.



Caution:

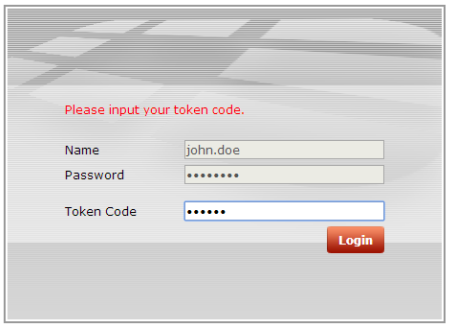
Do not select two-factor authentication at this point. The Two Factor Authentication is done externally on the FortiAuthenticator, so the FortiGate does not need to know it is happening. This is why the FortiAuthenticator is capable of authenticating FortiOS 4.2 and below and third party systems which have no direct support for two-factor authentication.

Testing

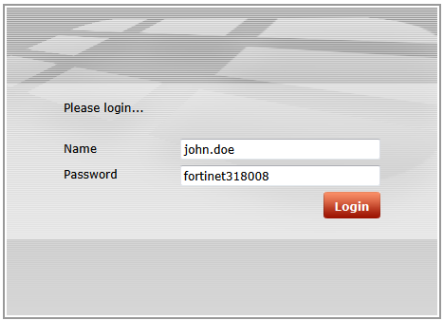
Attempt to log into the FortiGate Administration GUI using the john.doe credentials

```
Username:    john.doe
Password:    <password>
Token: <Token Passcode>
```

e.g.



It is also possible to authenticate using a concatenated passcode e.g. for a Password “fortinet” and one-time PIN of 318008, the login would become



However, obviously the password would be starred out.

Login via the will also be protected similarly e.g.

```
login as: john.doe
john.doe@192.168.0.254's password:
Remote Token:******
FortiGate01 #
```

Successful authentication will provide the user with access to the device with the correct permissions level based on their group membership and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
175	Fri Aug 19 14:12:51 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

Repeat the process with the jane.doe and unauthenticated.user who should obtain read –only and failed login, respectively.

If authentication is unsuccessful in any way, follow the steps in the Chapter **Appendix** A – Debugging to identify what is wrong.

Results

User	Permission granted
`john.doe`	super_admin (Super user permission)
`jane.doe`	roadmin (Read only admin)
`unauthenticated.user`	Login failed

RADIUS Packet Captures

RADIUS Query – john.doe

```
⊞ Frame 1: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
⊞ Ethernet II, Src: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: mpshrsv (1261), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5d (93)
    Length: 159
    Authenticator: 0593409ce190244907c47137627ae17f
    [The response to this request is in frame 4]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    ⊞ AVP: l=10  t=User-Name(1): john.doe
    ⊞ AVP: l=76  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=10  t=Acct-Session-Id(44): 00000049
    ⊞ AVP: l=13  t=Connect-Info(77): admin-login
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊞ VSA: l=6 t=Fortinet-Vdom-Name(3): root
```

RADIUS Response – john.doe

```
⊞ Frame 4: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.254 (192.168.0.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: mpshrsv (1261)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5d (93)
    Length: 200
    Authenticator: 48c597bd4716035068b7504d3c13b667
    [This is a response to a request in frame 1]
    [Time from request: 4.785145000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊟ AVP: l=21  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊞ VSA: l=15 t=Fortinet-Group-Name(1): RADIUS_Admins
```

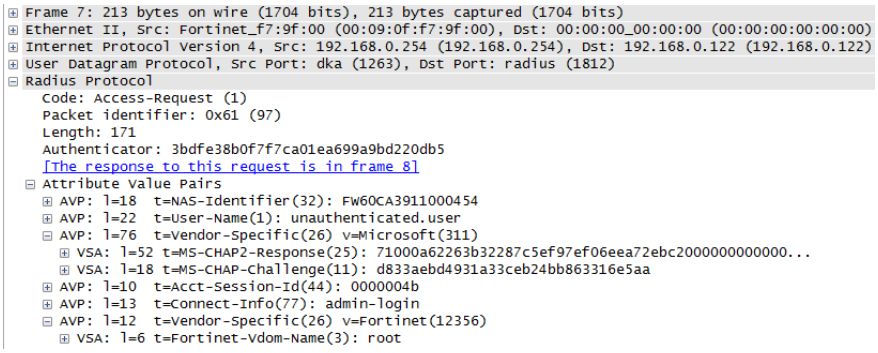
RADIUS Query – jane.doe

```
⊞ Frame 5: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
⊞ Ethernet II, Src: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: mpshrsv (1261), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5e (94)
    Length: 159
    Authenticator: 4ed0e19ddab8272d52e1a1272b228361
    [The response to this request is in frame 6]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    ⊞ AVP: l=10  t=User-Name(1): jane.doe
    ⊟ AVP: l=76  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=52 t=MS-CHAP2-Response(25): fd00d8cff98053acdbf3c5e366e8d19236d2000000000000...
      ⊞ VSA: l=18 t=MS-CHAP-Challenge(11): 1d09cc0d6d86a976b2ac72d7a754b5c7
    ⊞ AVP: l=10  t=Acct-Session-Id(44): 0000004a
    ⊞ AVP: l=13  t=Connect-Info(77): admin-login
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊞ VSA: l=6 t=Fortinet-Vdom-Name(3): root
```

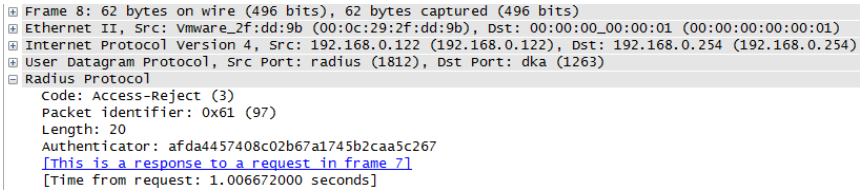
RADIUS Response – jane.doe

```
⊞ Frame 6: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.254 (192.168.0.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: mpshrsv (1261)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5e (94)
    Length: 200
    Authenticator: 559be2ba892dd950fc0bfb8e00774dac
    [This is a response to a request in frame 5]
    [Time from request: 0.020094000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=45 t=MS-CHAP2-Success(26): fd533d394136434444438303735424438393432454631414 1...
    ⊟ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=36 t=MS-MPPE-Recv-Key(17): b7377cd35550216f99d8a9b6b1252fe475a367fd1b3cb8b4...
    ⊟ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=36 t=MS-MPPE-Send-Key(16): be98565e22607199d4c32f3f4d9f25aebce3b0fb86d5c32d...
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=6 t=MS-MPPE-Encryption-Policy(7): Encryption-Allowed(1)
    ⊟ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
      ⊞ VSA: l=6 t=MS-MPPE-Encryption-Types(8): RC4-40-128(6)
    ⊟ AVP: l=21  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊞ VSA: l=15 t=Fortinet-Group-Name(1): RADIUS_Viewer
```

RADIUS Query – unauthenticated.user



RADIUS Response – unauthenticated.user



Attribute Defined Admin Users

Whilst it is possible to define assign users to groups, from which their administrative permissions are defined, it is also possible and more flexible to specify permissions via RADIUS Attributes. FortiAuthenticator can return specific RADIUS attributes based on the Group membership or directly from the user configuration. This section will describe the options available.

Configure additional test users

For this test, additional users are created to demonstrate the range and flexibility of options available Five RADIUS users were created each with different access rights configured via RADIUS attributes as follows:

```
User: rnone
      Attributes: None
User: ruser
      Attributes: Fortinet-Access-Profile = prof_admin
User: ronly
      Attributes: Fortinet-Access-Profile = read_only
User: radmin
      Attributes: Fortinet-Access-Profile = super_admin
```

Configure the Wildcard Admin User Object

In *System → Admin → Administrators*, select ***Create New***. In the resulting page, enter

```
Administrator:          RADIUS_Wildcard_Admins
Type:                   Remote
User Group:             RADIUS_Admins
Wildcard:               <enabled>
Admin Profile:          noaccess
```

Note we have created and assigned a new admin profile called *noaccess* which users will default to if they do not have a RADIUS Attribute profile override set.

To enable RADIUS Attribute overriding of the admin profile, the highlighted command must be set on the CLI (this feature is not available in the GUI)

```
config system admin
   edit "RADIUS_Wildcard_Admins"
        set remote-auth enable
        set accprofile "noaccess"
        set vdom "root"
        set wildcard enable
        set remote-group "radadmin"
        set radius-accprofile-override enable
   next
end
```

Testing

The following is the result of logging in with each of the assigned users:

User	Permission granted
rnone	noaccess
ruser	prof_admin
ronly	read_only
radmin	super_admin

Note.

FortiOS 5.0.7 currently only supports RADIUS Attribute Override when concatenating the token passcode at the end of the password. Challenge for token passcodes fails due to a bug. This is resolved in FortiOS 5.2.

RADIUS Packets

RADIUS Query – rnone

```
⊞ Frame 177: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
⊞ Ethernet II, Src: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
⊞ Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: fpo-fns (1066), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x24 (36)
    Length: 156
    Authenticator: 5babbf886767b18fe08336ca3668bab9
    [The response to this request is in frame 179]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    ⊟ AVP: l=7  t=User-Name(1): rnone
        User-Name: rnone
```

RADIUS Response – rnone

```
⊞ Frame 179: 221 bytes on wire (1768 bits), 221 bytes captured (1768 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.254 (192.168.0.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: fpo-fns (1066)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x24 (36)
    Length: 179
    Authenticator: 1b8ea31d3d7dd5c2555265c43789c53c
    [This is a response to a request in frame 177]
    [Time from request: 0.021746000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
```

RADIUS Query – ronly

```
⊞ Frame 17: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
⊞ Ethernet II, Src: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
⊞ Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: polestar (1060), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1a (26)
    Length: 156
    Authenticator: d65f3e15adb78cbd01dccecc2e6939a8
    [The response to this request is in frame 19]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    ⊟ AVP: l=7  t=User-Name(1): ronly
        User-Name: ronly
```

RADIUS Response – ronly

```
⊞ Frame 19: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.254 (192.168.0.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: polestar (1060)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1a (26)
    Length: 196
    Authenticator: c7906ce252dd7b1ecff538f53f95185a
    [This is a response to a request in frame 17]
    [Time from request: 0.022597000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊟ AVP: l=17  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊟ VSA: l=11 t=Fortinet-Access-Profile(6): read_only
          Fortinet-Access-Profile: read_only
```

RADIUS Query – radmin

```
⊞ Frame 50: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
⊞ Ethernet II, Src: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
⊞ Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: veracity (1062), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x1d (29)
    Length: 157
    Authenticator: 455e7a5bd76f8873426aeb762bd5c038
    [The response to this request is in frame 53]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    ⊟ AVP: l=8  t=User-Name(1): radmin
        User-Name: radmin
```

RADIUS Response – radmin

```
⊞ Frame 80: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Fortinet_f7:9f:00 (00:09:0f:f7:9f:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.254 (192.168.0.254)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: veracity (1062)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x1e (30)
    Length: 198
    Authenticator: e46a93bdc13618efedf36e9876c296e0
    [This is a response to a request in frame 78]
    [Time from request: 0.040102000 seconds]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊞ AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    ⊟ AVP: l=19  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊟ VSA: l=13 t=Fortinet-Access-Profile(6): super_admin
          Fortinet-Access-Profile: super_admin
```

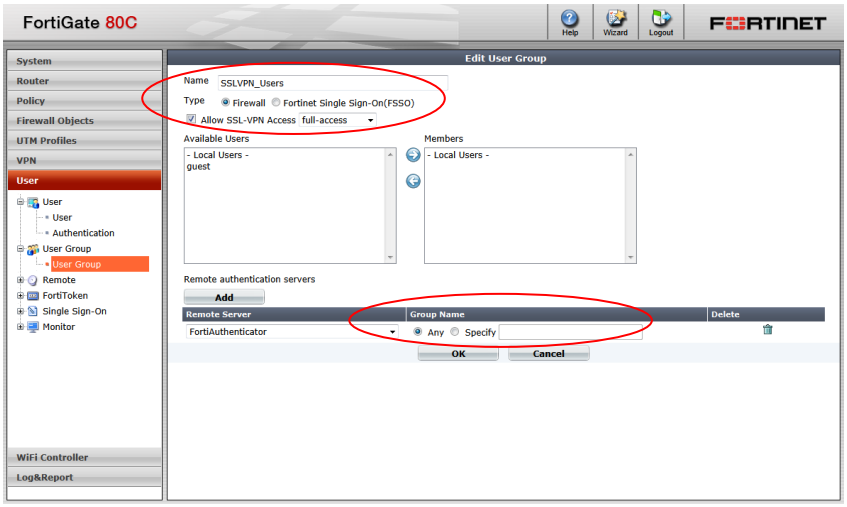
FortiGate (SSL-VPN Users)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

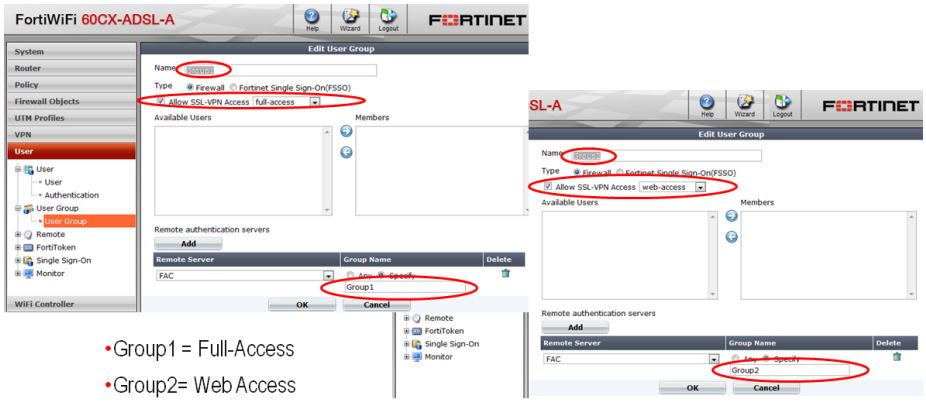
Note. This guide does not detail how to configure the SSL-VPN, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the SSL-VPN please see the SSL-VPN Guide for your specific firmware release here http://docs.fortinet.com/fgt.htm.

Create User Group

In *User → User Group*, select *Create New*. Create a group called *SSLVPN_Users* of *type firewall* and enable “Allow SSL-VPN Access” with your selected access permissions. Under *Remote Authentication Servers*, click ***Add***. Select *FortiAuthenticator* from the drop down list and click ***OK*** to save.



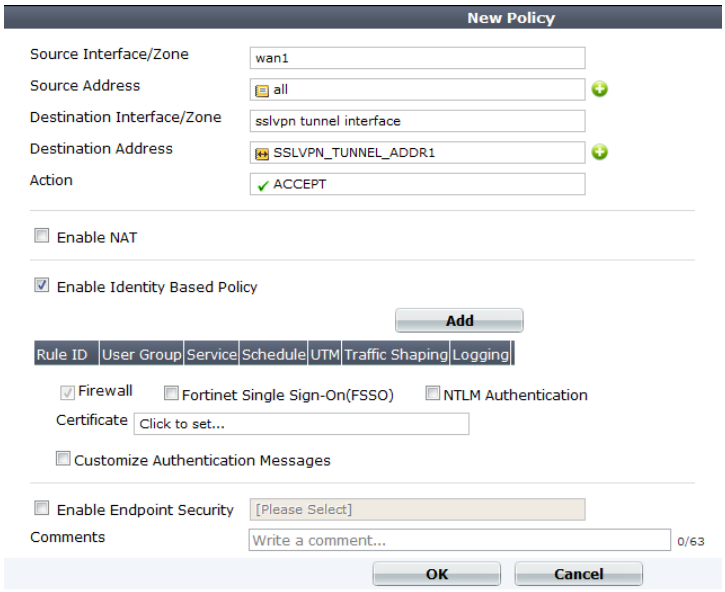
The Group Name configuration can be used to limit which users can authenticate or to limit what they can do in the VPN (by creating multiple groups in conjunction with the Allow SSL-VPN Access option).



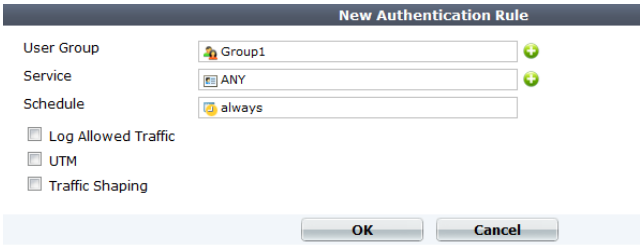
Firewall SSL VPN Policy

Create a firewall policy which enables SSL-VPN access into you chosen network. In this example, a policy is being created from WAN1 to the Internal network for the defined Group.

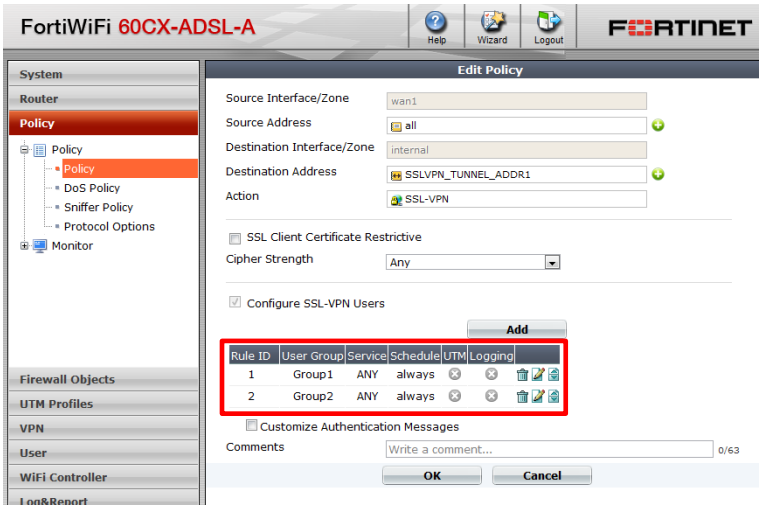
Browse to *Policy* → *Policy* and select ***Create New***. Select *Source Interface*: WAN1, *Destination Interface*: Internal and Action: SSL-VPN.



Enable *Identity Based Policy* and Add the all the User Groups allowed to log into the SSLVPN.



Select the *required Group* from the Available. Select Any from the Available Services. Click ***OK*** and ***OK*** again on the *Edit Policy page* to save the settings. Where multiple user groups have been configured to allow differentiated VPN access, specify all user groups at this point e.g



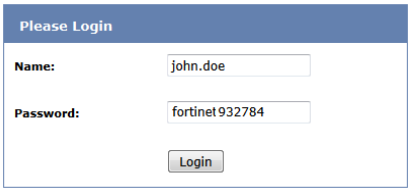
User Login – Password + Token PIN Appended

Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (dependent on your settings) with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

`Username:` ***`john.doe`***

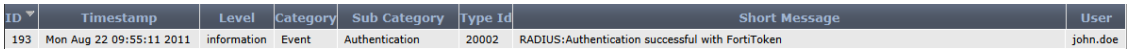
`Password:` **`<password><Token PIN>`**

e.g. for a Password "fortinet" and one-time PIN of 318008, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator



If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

User Login – Token PIN Challenge

Whilst the PIN Appended method is the most widely supported method of authentication for 3rd party systems, FortiGate SSL VPN supports the RADIUS Challenge-Response mechanism. This allows the user to enter their username and password and then be challenged separately for the token PIN which is more intuitive. No changes need to be made to the systems to support either method and they can be used interchangeably.

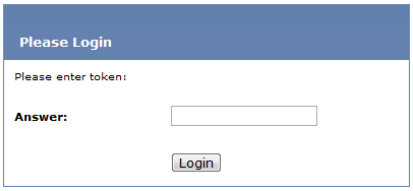
Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (dependent on your settings) with your new credentials.

```
Username:    john.doe
Password:    <password><Token PIN>
```

e.g. for a Password “fortinet”, the login would become

However obviously the password would be starred out.

The FortiAuthenticator will detect that the password is correct but the token PIN has not been provided and issue a RADIUS Challenge. FortiGate detects this and prompts the user for the additional detail.



The user should enter the correct token PIN and click login.

Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

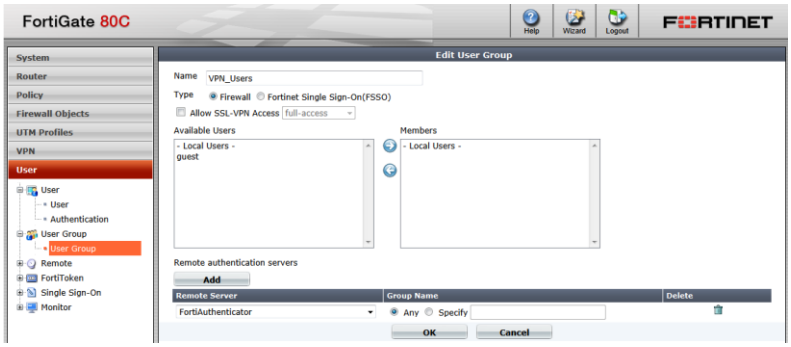
IPSec VPN

Note that this guide does not detail how to configure the IPSec VPN or the FortiClient Connect client, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the VPN on FortiGate and the Forticlient Connect client please see the relevant documentation here http://docs.fortinet.com/fgt.html.

This section assumes you have a working IKE configuration.

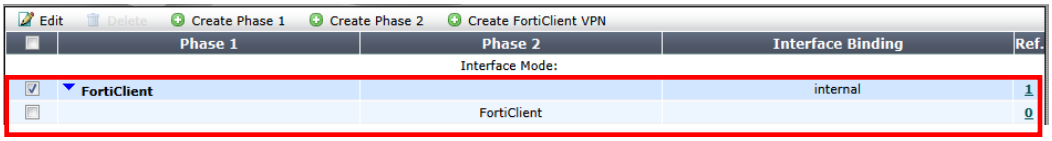
Create User Group

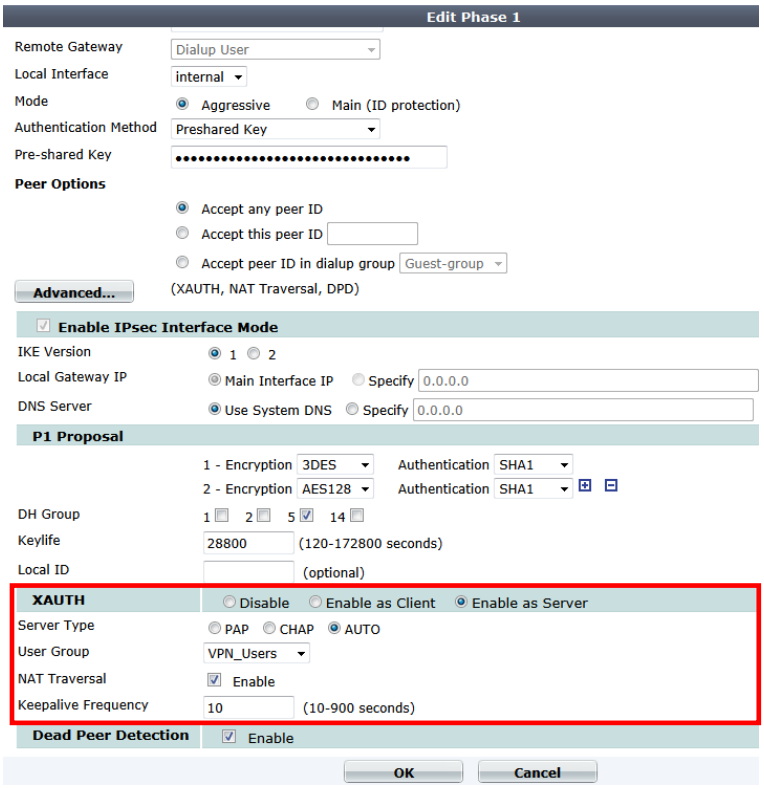
In *User → User Group*, select ***Create New***. Create a group called *VPN_Users* of *type firewall* and. Under *Remote Authentication Servers*, click *Add*. Select *FortiAuthenticator* from the drop down list and click *OK* to save.



Edit Existing IKE Policy

To enable FortiAuthenticator strong two-factor authentication, the existing IKE Policy must be configured to enable XAUTH (eXtended AUTHentication). To do this browse to VPN → IPSec → Auto Key (IKE) and Edit the Phase 1 settings of your VPN (select the radio button of the first entry for your VPN and click Edit)





FortiManager (Admin Users)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

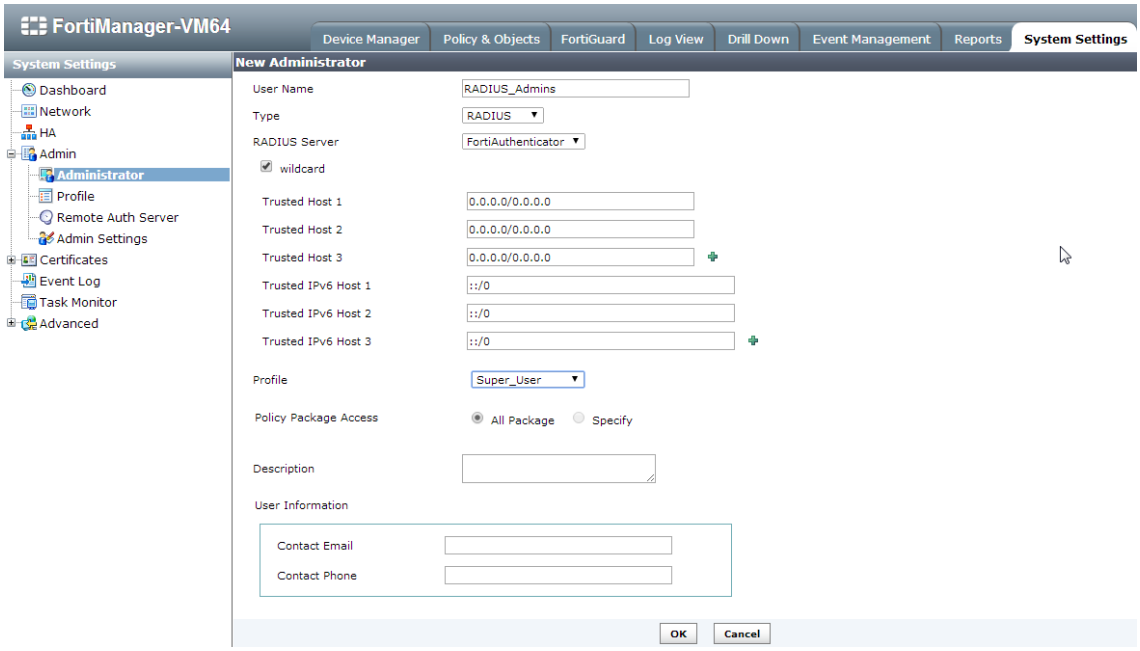
Log into the FortiManager GUI and browse to *System Settings → Admin → Remote Auth Server*. Select **Create New** and **RADIUS**.

Enter the details of the remote FortiAuthenticator including the shared secret.

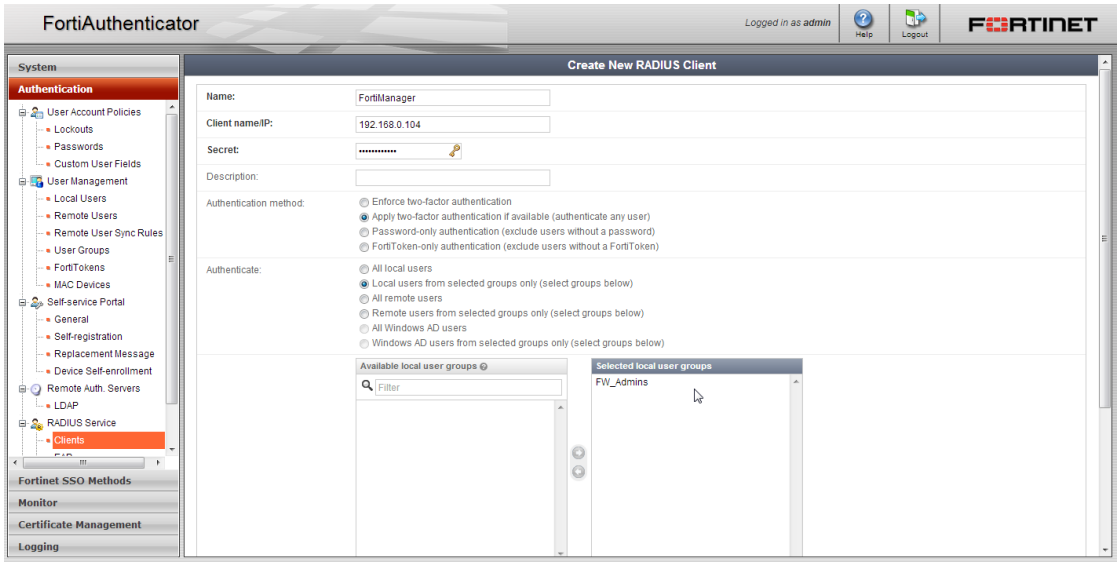
Create the Admin Users

In *System Settings → Admin → Administrator*, select ***Create New***. Enter a name for the config; if this is for a single admin user, enter the user name, if this is for multiple users, enter a generic name and select Wildcard.

Select *Auth Type RADIUS* and select the RADIUS Server you created in the previous step.



Wildcard authentication will allow authentication from any account on the FortiAuthenticator. To restrict authentication, RADIUS Service Clients can be configured to only authenticate specific user groups.



Access Profile Override

FortiManager supports the radius-accprofile-override CLI command to allow RADIUS AVPs specified in the RADIUS Access-Accept packet to elevate admin privilege.

```
config system admin user
    edit "RADIUS_Admins"
        set profileid "noaccess"
            set adom "all adoms"
            set policy-package "all_policy_packages"
        set user type radius
        set radius_server "FortiAuthenticator"
            config meta-data
                edit "Contact Email"
                next
```

```
                edit "Contact Phone"
                next
            end
        set wildcard enable
        set radius-accprofile-override enable
    next
end
```

Once enabled, the default access profile (noaccess above) can be overridden by specifying the following RADIUS Attribute Value Pair (AVP) in the Access-Accept packet.

```
Fortinet-Access-Profile = <value>
```

Where <value> = a string which matches the name of an Access profile defined on the FortiManager under System → Admin -> Access Profile.

Testing

Attempt to log into the FortiManager GUI with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

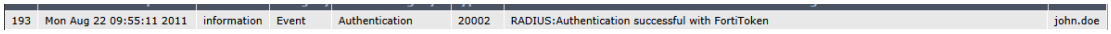
Username: ***john.doe***

Password: **<password><Token PIN>**

e.g. for a Password "fortinet" and one-time PIN of 561555, the login would become

However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator

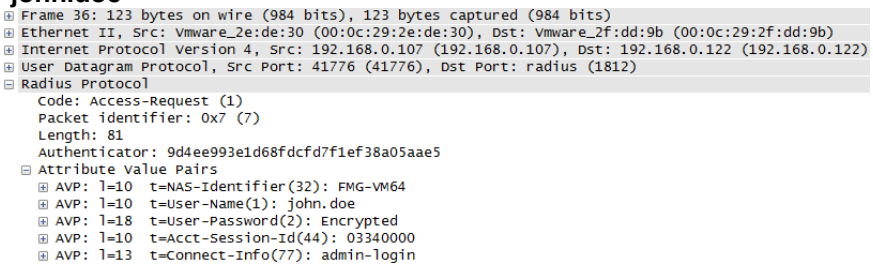


If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

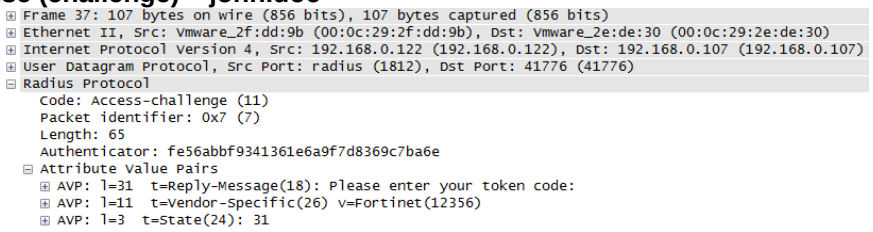
Note: Up to FortiManager 5.0.6, RADIUS Challenge Response was not supported so the token appending method should be used. This has been resolved in FortiManager 5.0.7 and 5.2.

RADIUS Packets

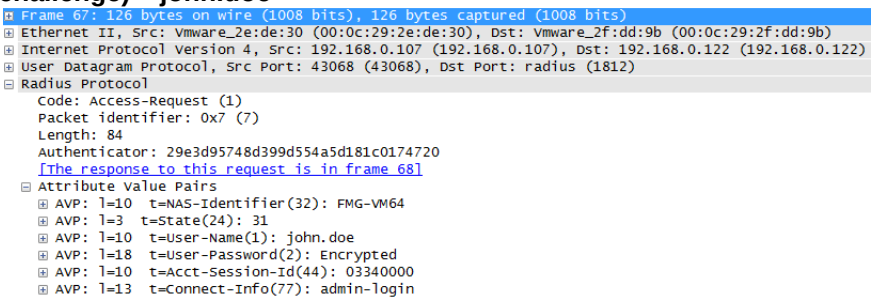
RADIUS Query – john.doe



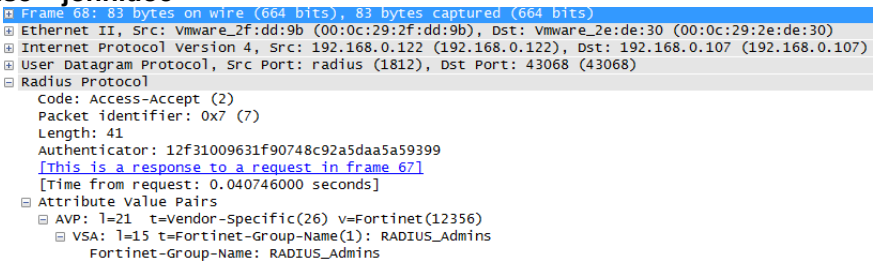
RADIUS Response (challenge) – john.doe



RADIUS Query (challenge) – john.doe



RADIUS Response – john.doe



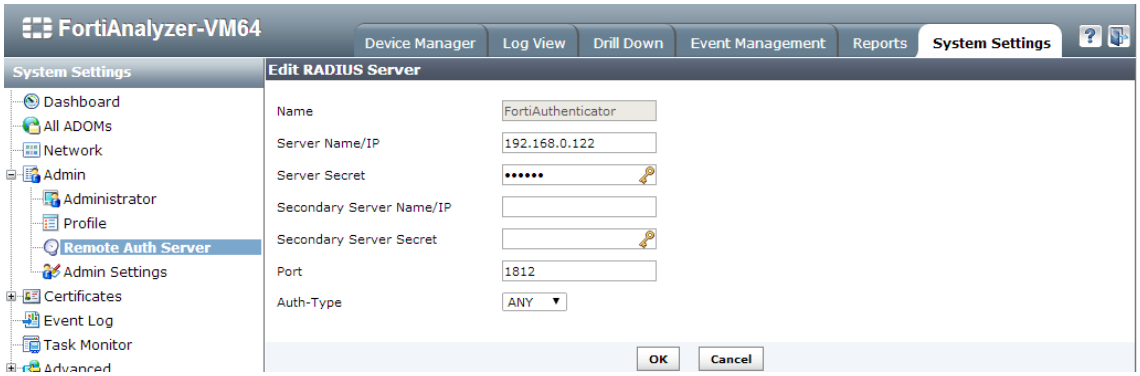
FortiAnalyzer (Admin Users)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the FortiAnalyzer GUI and browse to *System Settings → Admin → Remote Auth Server*. Select **Create New** and **RADIUS**.

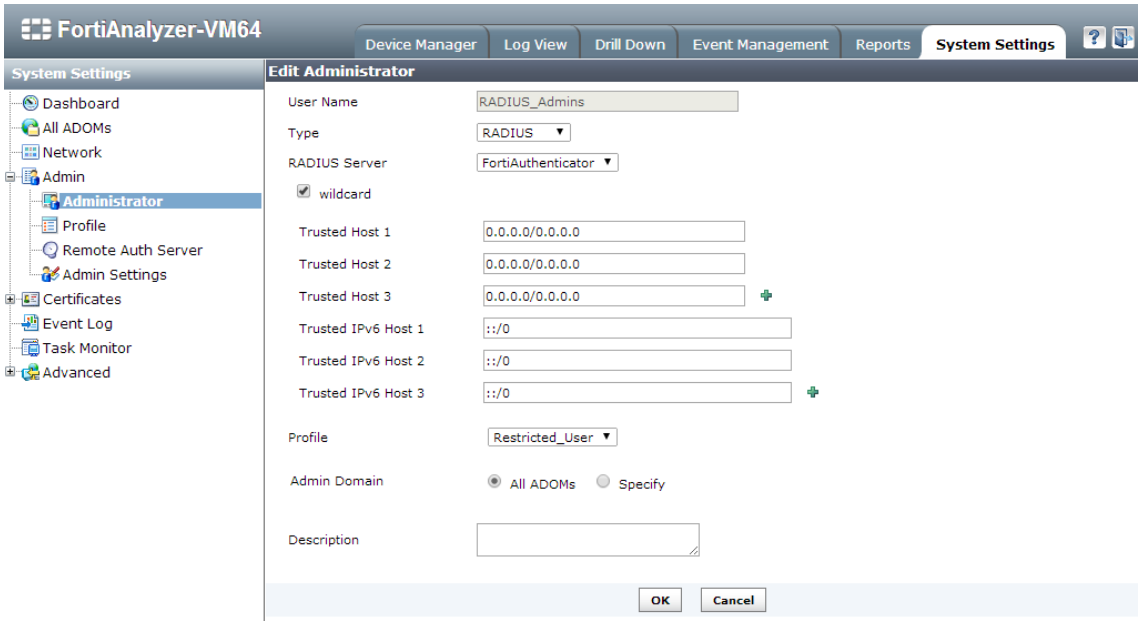
Enter the details of the remote FortiAuthenticator including the shared secret.



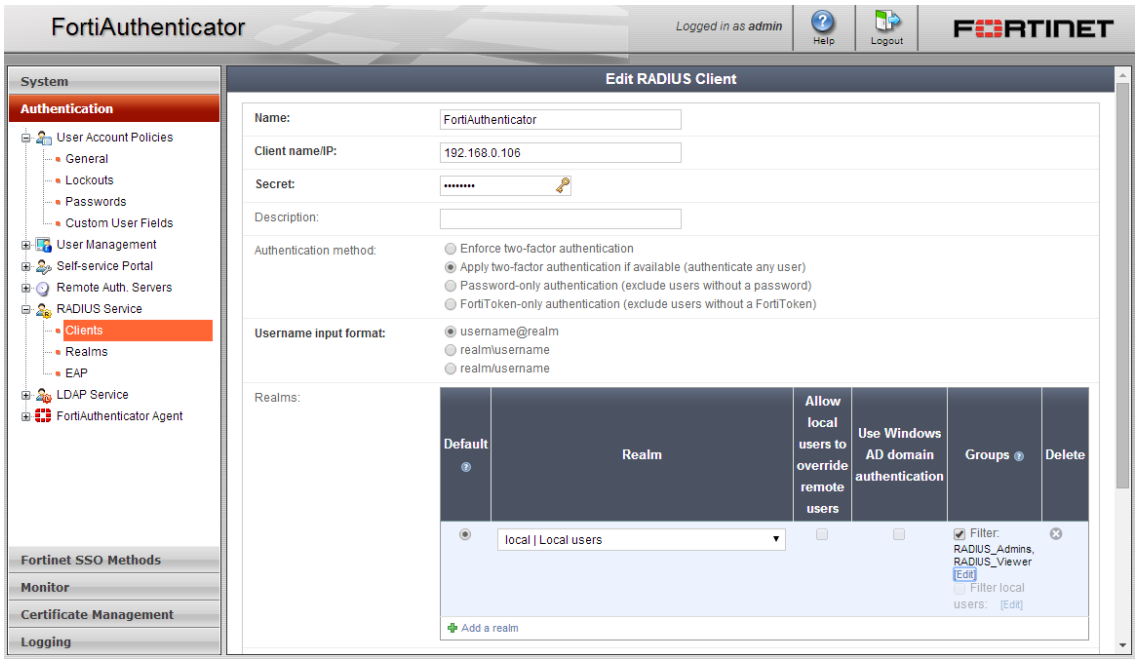
Create the Admin Users

In *System Settings → Admin → Administrator*, select ***Create New***. Enter a name for the config; if this is for a single admin user, enter the user name, if this is for multiple users, enter a generic name and select Wildcard.

Select ***Auth Type RADIUS*** and select the RADIUS Server you created in the previous step.



Wildcard authentication will allow authentication from any account on the FortiAuthenticator. To restrict authentication, RADIUS Service Clients can be configured to only authenticate specific user groups.



Access Profile Override

FortiAnalyzer supports the radius-accprofile-override CLI command to allow RADIUS AVPs specified in the RADIUS Access-Accept packet to elevate admin privilege.

```
config system admin user
    edit "RADIUS Admins"
        set profileid "noaccess"
            set adom "all adoms"
            set policy-package "all_policy_packages"
        set user_type radius
```

```
        set radius server "FortiAuthenticator"
        set wildcard enable
        set radius-accprofile-override enable
    next
end
```

Once enabled, the default access profile (noaccess above) can be overridden by specifying the following RADIUS Attribute Value Pair (AVP) in the Access-Accept packet.

```
Fortinet-Access-Profile = <value>
```

Where <value> = a string which matches the name of an Access profile defined in System → Admin -> Access Profile.

Testing

Attempt to log into the FortiAnalyzer GUI with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

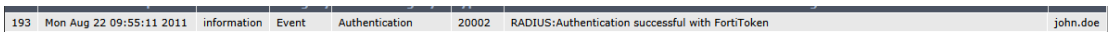
Username: ***john.doe***

Password: **<password><Token PIN>**

e.g. for a Password "fortinet" and one-time PIN of 561555, the login would become

However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiAnalyzer and will generate a login event log on the FortiAuthenticator



If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Note: Up to FortiManager 5.0.6, RADIUS Challenge Response was not supported so the token appending method should be used This has been resolved in FortiManager 5.0.7 and 5.2.

RADIUS Packets

RADIUS Query – john.doe

```
⊞ Frame 36: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
⊞ Ethernet II, Src: Vmware_2e:de:30 (00:0c:29:2e:de:30), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
⊞ Internet Protocol Version 4, Src: 192.168.0.107 (192.168.0.107), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: 41776 (41776), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x7 (7)
    Length: 81
    Authenticator: 9d4ee993e1d68fdcfd7f1ef38a05aae5
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=10  t=NAS-Identifier(32): FMG-VM64
    ⊞ AVP: l=10  t=User-Name(1): john.doe
    ⊞ AVP: l=18  t=User-Password(2): Encrypted
    ⊞ AVP: l=10  t=Acct-Session-Id(44): 03340000
    ⊞ AVP: l=13  t=Connect-Info(77): admin-login
```

RADIUS Response (challenge) – john.doe

```
⊞ Frame 37: 107 bytes on wire (856 bits), 107 bytes captured (856 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Vmware_2e:de:30 (00:0c:29:2e:de:30)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.107 (192.168.0.107)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 41776 (41776)
⊟ Radius Protocol
    Code: Access-challenge (11)
    Packet identifier: 0x7 (7)
    Length: 65
    Authenticator: fe56abbf9341361e6a9f7d8369c7ba6e
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=31  t=Reply-Message(18): Please enter your token code:
    ⊞ AVP: l=11  t=Vendor-Specific(26) v=Fortinet(12356)
    ⊞ AVP: l=3  t=State(24): 31
```

RADIUS Query (challenge) – john.doe

```
⊞ Frame 67: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
⊞ Ethernet II, Src: Vmware_2e:de:30 (00:0c:29:2e:de:30), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
⊞ Internet Protocol Version 4, Src: 192.168.0.107 (192.168.0.107), Dst: 192.168.0.122 (192.168.0.122)
⊞ User Datagram Protocol, Src Port: 43068 (43068), Dst Port: radius (1812)
⊟ Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x7 (7)
    Length: 84
    Authenticator: 29e3d95748d399d554a5d181c0174720
    [The response to this request is in frame 68]
  ⊟ Attribute Value Pairs
    ⊞ AVP: l=10  t=NAS-Identifier(32): FMG-VM64
    ⊞ AVP: l=3  t=State(24): 31
    ⊞ AVP: l=10  t=User-Name(1): john.doe
    ⊞ AVP: l=18  t=User-Password(2): Encrypted
    ⊞ AVP: l=10  t=Acct-Session-Id(44): 03340000
    ⊞ AVP: l=13  t=Connect-Info(77): admin-login
```

RADIUS Response – john.doe

```
⊞ Frame 68: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
⊞ Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Vmware_2e:de:30 (00:0c:29:2e:de:30)
⊞ Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.107 (192.168.0.107)
⊞ User Datagram Protocol, Src Port: radius (1812), Dst Port: 43068 (43068)
⊟ Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7 (7)
    Length: 41
    Authenticator: 12f31009631f90748c92a5daa5a59399
    [This is a response to a request in frame 67]
    [Time from request: 0.040746000 seconds]
  ⊟ Attribute Value Pairs
    ⊟ AVP: l=21  t=Vendor-Specific(26) v=Fortinet(12356)
      ⊟ VSA: l=15 t=Fortinet-Group-Name(1): RADIUS_Admins
          Fortinet-Group-Name: RADIUS_Admins
```

FortiWeb (Admin Users)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

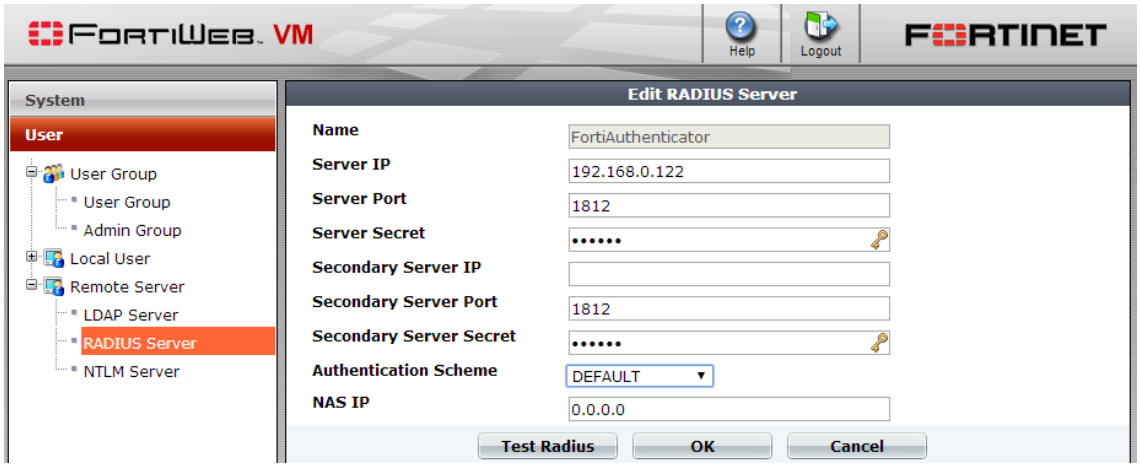
Note:

The current FortiWeb version 5.2.1 does not support challenge-response so the Token-Appended method should be used.

Configure the RADIUS Server

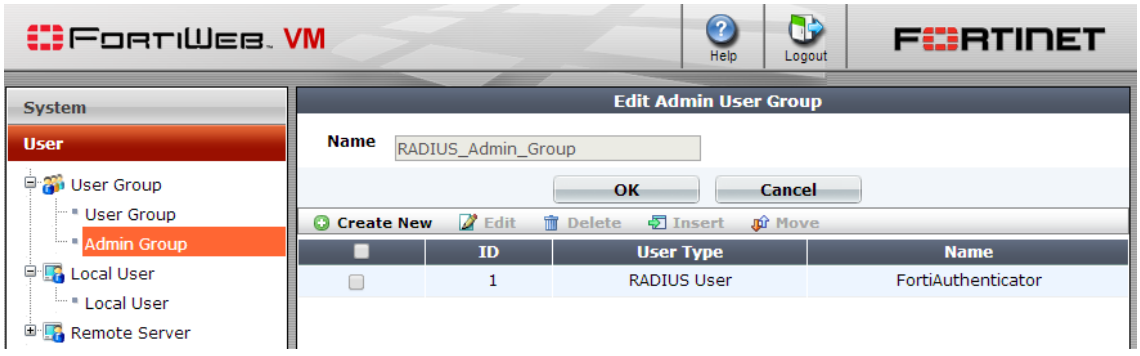
Log into the FortiWeb GUI and browse to *User → Remote Server → RADIUS Server* and Select ***Create New***.

Enter the details of the remote FortiAuthenticator including the shared secret.



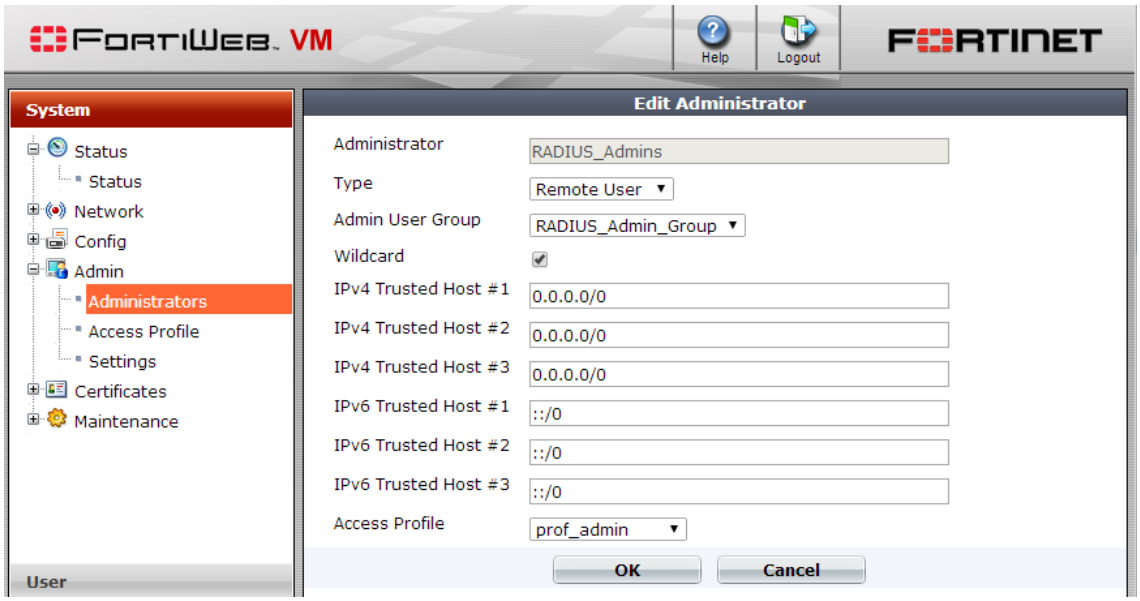
Create an Admin Group

In *User → Admin Group*, select ***Create New***. Enter the Auth Type RADIUS and select the RADIUS Server you created in the previous step under the heading user.



Create an Admin User

Browse to *System → Admin → Administrators*, select ***Create New***. Enter the details of the user to be authenticated, the type (Remote User), the Admin User Group (as created in the previous step) and the access profile to use.



Access Profile Override

Similar to FortiGate, FortiWeb supports the accprofile-override CLI command to allow RADIUS AVPs specified in the RADIUS Access-Accept packet to elevate admin privilege.

```
config system admin
  edit "RADIUS Admins"
    set access-profile noaccess
    set type remote-user
    set admin-usergrp RADIUS_Admin_Group
    set wildcard enable
    set accprofile-override enable
  next
end
```

Once enabled, the default access profile (noaccess above) can be overridden by specifying the following RADIUS Attribute Value Pair (AVP) in the Access-Accept packet.

```
Fortinet-Access-Profile = <value>
```

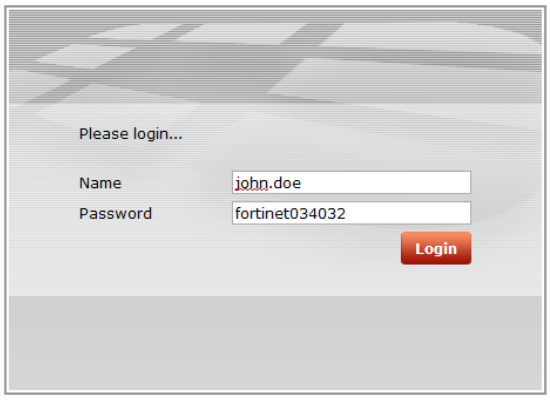
Where <value> = a string which matches the name of an Access profile defined in System → Admin -> Access Profile.

Testing

Attempt to log into the FortiWeb GUI e.g. https://192.168.1.99 (dependent on your settings) with the FortiAuthenticator credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username:   john.doe
Password:   <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 034032, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiWeb and will generate a login event log on the FortiAuthenticator

#	Date	Time	Level	User Interface	Action	Message
1	2014-06-20	04:47:16		GUI	login	User john.doe(RADIUS_Admins) login successfully from GUI(192.168.0.156)

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

RADIUS Packets

RADIUS Query – john.doe

```
Frame 72: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
Ethernet II, Src: Vmware_8e:fd:c0 (00:0c:29:8e:fd:c0), Dst: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b)
Internet Protocol Version 4, Src: 192.168.0.101 (192.168.0.101), Dst: 192.168.0.122 (192.168.0.122)
User Datagram Protocol, Src Port: 20954 (20954), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x6f (111)
    Length: 116
    Authenticator: 9ae3863f7a05ff5d3583b72cd84f8b44
    [The response to this request is in frame 73]
  Attribute Value Pairs
    AVP: l=10  t=NAS-Identifier(32): FortiWeb
    AVP: l=10  t=User-Name(1): john.doe
    AVP: l=76  t=Vendor-Specific(26) v=Microsoft(311)
```

RADIUS Response – john.doe

```
Frame 73: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
Ethernet II, Src: Vmware_2f:dd:9b (00:0c:29:2f:dd:9b), Dst: Vmware_8e:fd:c0 (00:0c:29:8e:fd:c0)
Internet Protocol Version 4, Src: 192.168.0.122 (192.168.0.122), Dst: 192.168.0.101 (192.168.0.101)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 20954 (20954)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x6f (111)
    Length: 200
    Authenticator: 9b3ba321c65cbad58b7b08b1333727cb
    [This is a response to a request in frame 72]
    [Time from request: 0.040654000 seconds]
  Attribute Value Pairs
    AVP: l=51  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=42  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=12  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=21  t=Vendor-Specific(26) v=Fortinet(12356)
      VSA: l=15 t=Fortinet-Group-Name(1): RADIUS_Admins
```

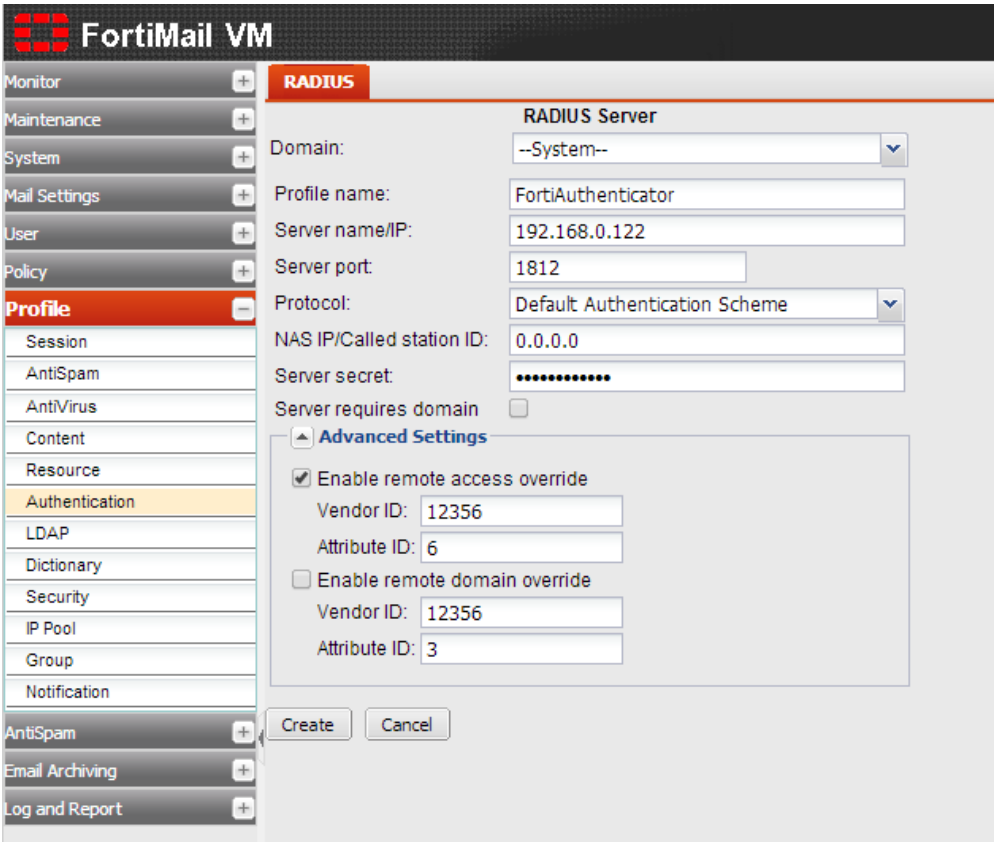
FortiMail (Admin Auth)

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration". Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the FortiMail GUI and browse to *Profile → Authentication*. Select ***New***.

Enter the details of the remote FortiAuthenticator including the FortiAuthenticator IP, Authentication Port (1812), Port, Protocol (authentication scheme) and shared secret.

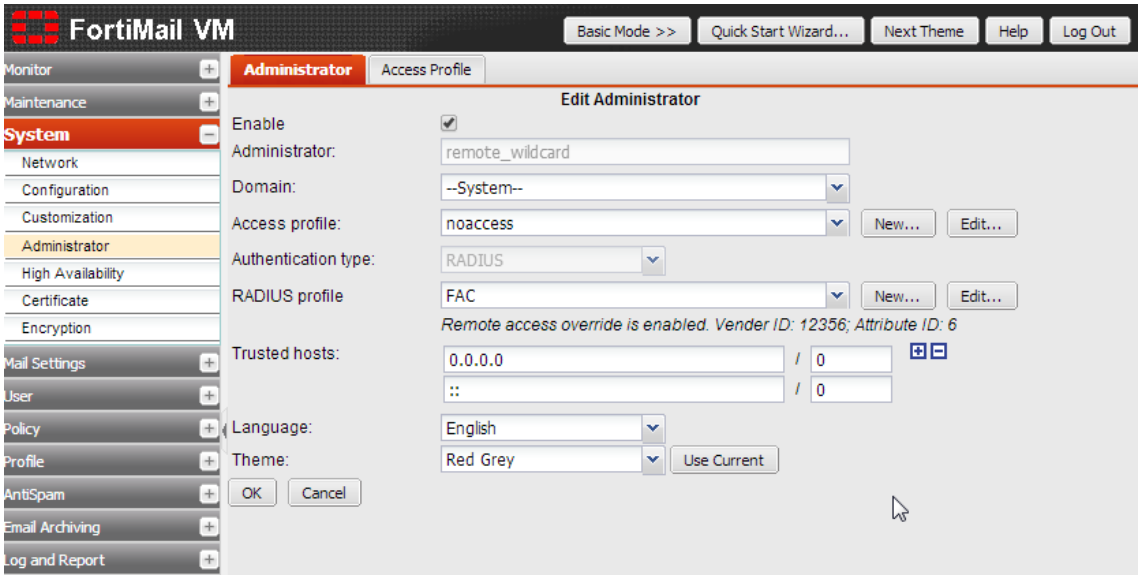


In *System → Administrator*, select ***New***. Enter the user name, Auth Type RADIUS and select the RADIUS Server you created in the previous step.

In this example, Remote Access Override is enabled for Vendor ID = 12356 and Attribute ID = 6. This corresponds to the attribute *Fortinet-Group-Name* in the Fortinet RADIUS dictionary.

Create the Admin User

FortiMail has a predefined wildcard user (remote_wildcard) where any user on the remote authentication server is authenticated. In this example, the Access Profile is set to “noaccess” however, the user override can be used to escalate privileges.



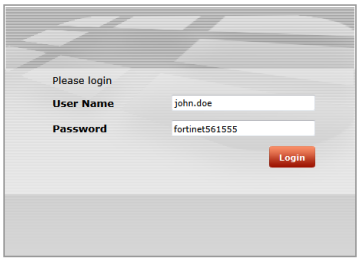
Admin User Logon

Attempt to log into the FortiMail GUI e.g. https://192.168.1.99 (dependent on your settings) with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

`Username:` ***john.doe***

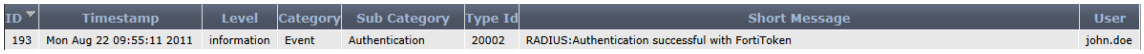
`Password:` **<password><Token PIN>**

e.g. for a Password “fortinet” and one-time PIN of 561555, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator



ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

Cisco IOS based switches and routers

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The following was tested with a Cisco 2950 switch running IOS 12.1(13). Whilst this should work with other versions and IOS based routers, the command structure on the Cisco IOS is liable to vary between versions so please consult the Cisco documentation for changes.

Telnet Authentication

Configure the Cisco switch to allow remote access via Telnet. To do this enter enable mode on the switch and execute conf t to begin editing the config:

```
Switch> en
Enter Password: *********
Switch# conf t
Switch(config)#
```

Enter the following commands to enable an IP address on the switch and enable telnet management

```
Switch(config)# interface Vlan1
Switch(config)# ip address 192.168.0.253 255.255.255.0
Switch(config)# ip default-gateway 192.168.0.1
Switch(config)# no shutdown
```

Enter the following commands to enable two-factor authentication

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# radius-server host 192.168.0.122 auth-port 1812 key fortinet1234
Switch(config)# radius-server retransmit 3
```

Attempt to log in to the switch via telnet and you should be presented with a two-factor enhanced login e.g.

```
telnet 192.168.0.253
User Access Verification
Username: john.doe
Password: fortinet
Please enter token:721194
Switch>
```

Notice that the login has dropped the user into the non privileged admin level denoted by the >. Enable mode is accessed via the command ***enable*** and entering the enable password.

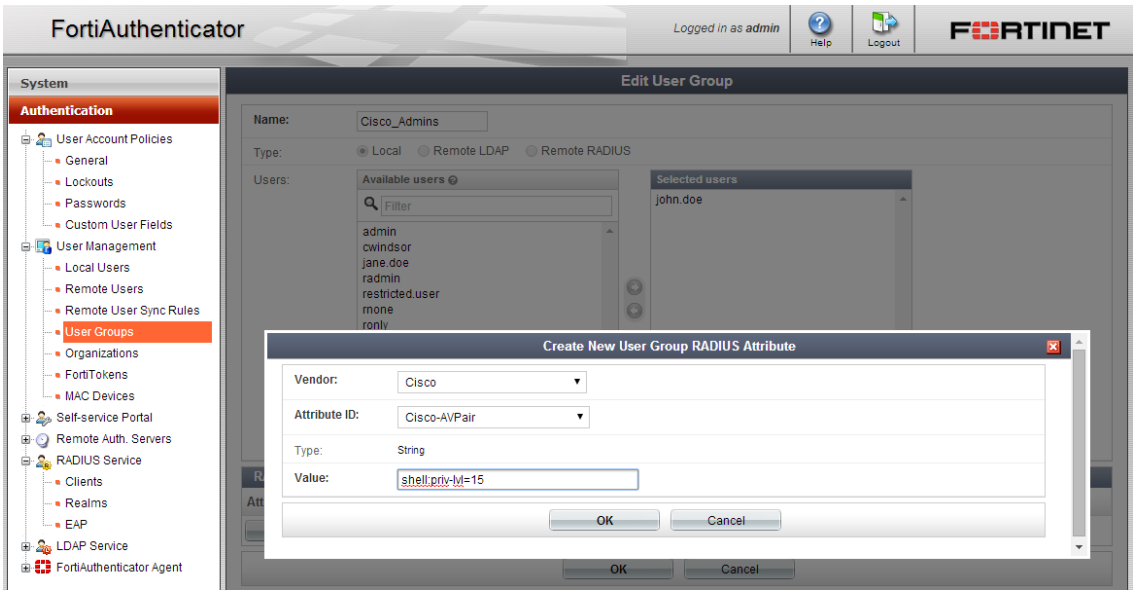
Configure Enable Authorization

To directly authenticate the user into enable mode, it is possible to include an authorization attribute in the RADIUS Access-Accept packet. Cisco uses the following attribute from their standard RADIUS Dictionary for this purpose:

```
Cisco-AVPair = shell:priv-lvl=15
```

RADIUS Attributes can be configured either at the group or user level. The following example sets this attribute at the group level but the configuration mechanism is the same for both.

- Browse to *Authentication* → *User Groups* → *Local* and create a new group called ***Cisco_Admins***. Add the required users to this group.
- Edit the Group and select *Add Attributes*.
- Select the *Vendor* ***Cisco*** and *Attribute-ID* ***Cisco-AV-Pair***
- In the *Attribute Value* field enter shell:priv-lvl=15 which specifies to give full administrative rights to the user.



Create a second Attribute with *Vendor* ***Default*** (this is the RADIUS RFC standard dictionaries), *Attribute-ID* ***Service-Type*** and *Attribute Value* ***NAS-Prompt-User***.

To configure the switch to accept these attributes to escalate admin privilege, enter the following configuration.

```
Switch(config)#aaa authorization exec default radius
```

Attempt to login again

```
telnet 192.168.0.253
User Access Verification
Username: john.doe
Password: fortinet
Please enter token:983403
Switch#
```

Notice that the user is granted the enable (15) privilege level denoted by #.

Privilege Levels

The default Cisco IOS privilege levels are defined as:

Privilege Level	Result
0	Seldom used, but includes five commands: disable, enable, exit, help, and logout
1	User level only (prompt is switch>). The default level for login
15	Privileged level (prompt is router#), the level after going into enable mode

Whilst authorization levels 0, 1 and 15 are configured by default, levels 2 to 14 are undefined and can be used to create additional levels by adding and removing specific CLI commands e.g.

To specify which commands will exist in privilege level 7, issue the following commands on Switch1 from the console:

```
Switch1(config)# privilege configure level 7 snmp-server host
Switch1 (config)# privilege configure level 7 snmp-server enable
Switch1 (config)# privilege configure level 7 snmp-server
Switch1 (config)# privilege exec level 7 ping
Switch1 (config)# privilege exec level 7 configure terminal
Switch1 (config)# privilege exec level 7 configure
```

This level can be then authorized by creating a separate FortiAuthenticator group, including the required users and specifying the new RADIUS Attribute privilege level e.g.

```
Cisco-AVPair = shell:priv-lvl=7
```

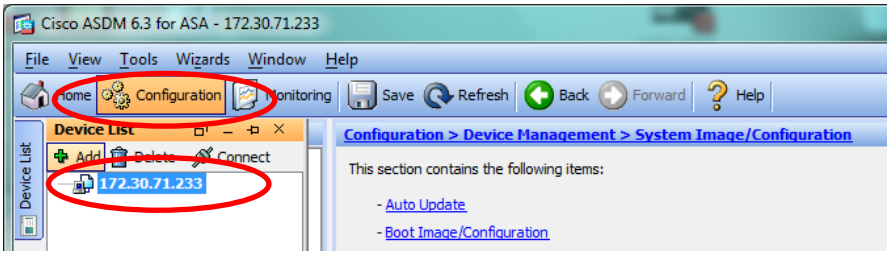
Cisco ASA

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The following was tested with a Cisco ASA 5520 running ASA version 8.2(1) and ASDM 6.3(5). Whilst this should work with other ASA versions, Cisco firmware is liable to vary between versions so please consult the Cisco documentation for changes. The configuration of the Cisco ASA device requires the installation of the ASDM management software and/or Oracle Java.

Configuring System Authentication

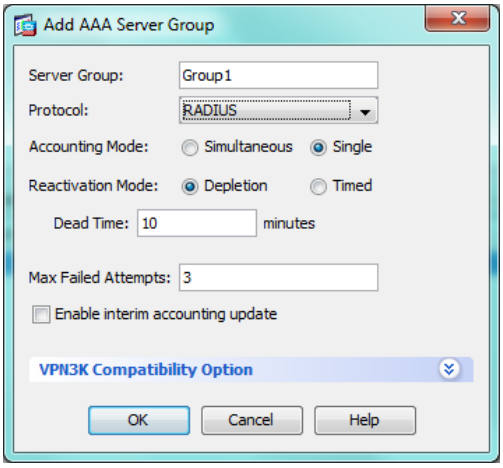
Select the relevant ASA device in Device List and then Configuration from top menu.



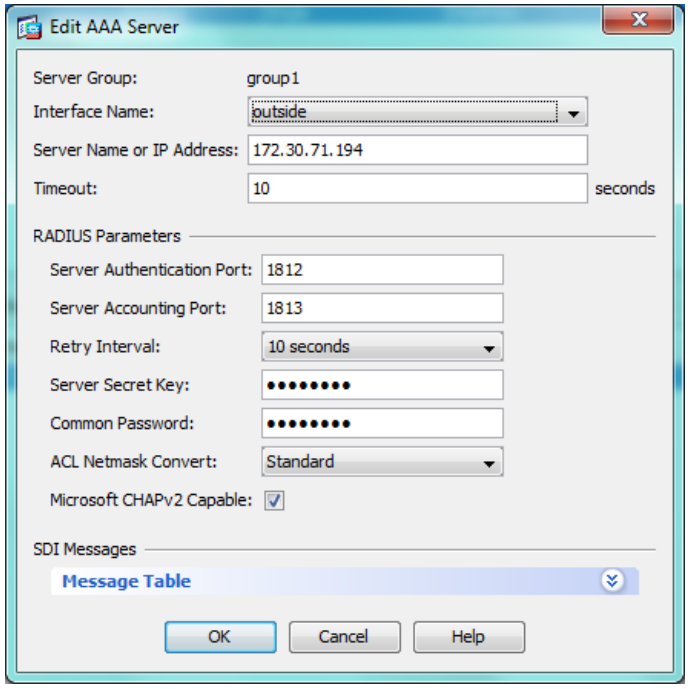
In Device Management, browse to Users/AAA → AAA Server Groups.

Under AAA Server Groups click Add.

Create a group into which the FortiAuthenticator device will later be added as shown and click OK.

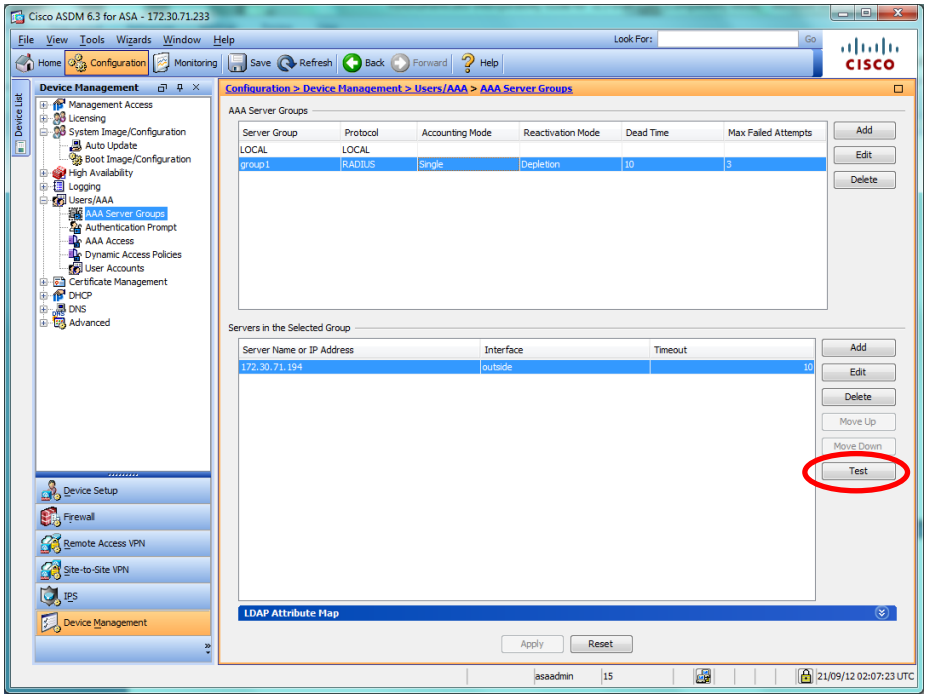


- Select the Server Group specified in the previous step and, in the Servers in Selected Group window, *click **Add***
- Specify the details of the FortiAuthenticator device as shown, taking care to include the correct Pre-Shared Key (Server Secret Key)



- Once complete, *select* ***OK***.

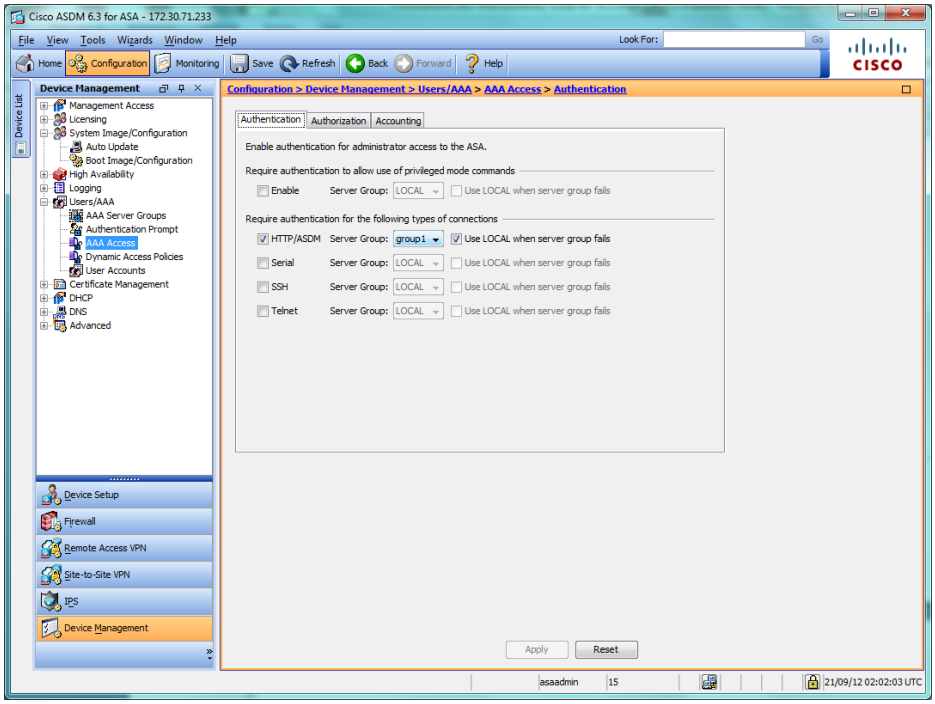
The configuration can be validated by selection the group and the FortiAuthenticator server and selecting ***Test.***



To configure authentication of the Cisco ASA system via FortiAuthenticator two-factor authentication:

- Browse to Device Management → Users/AAA → AAA Access

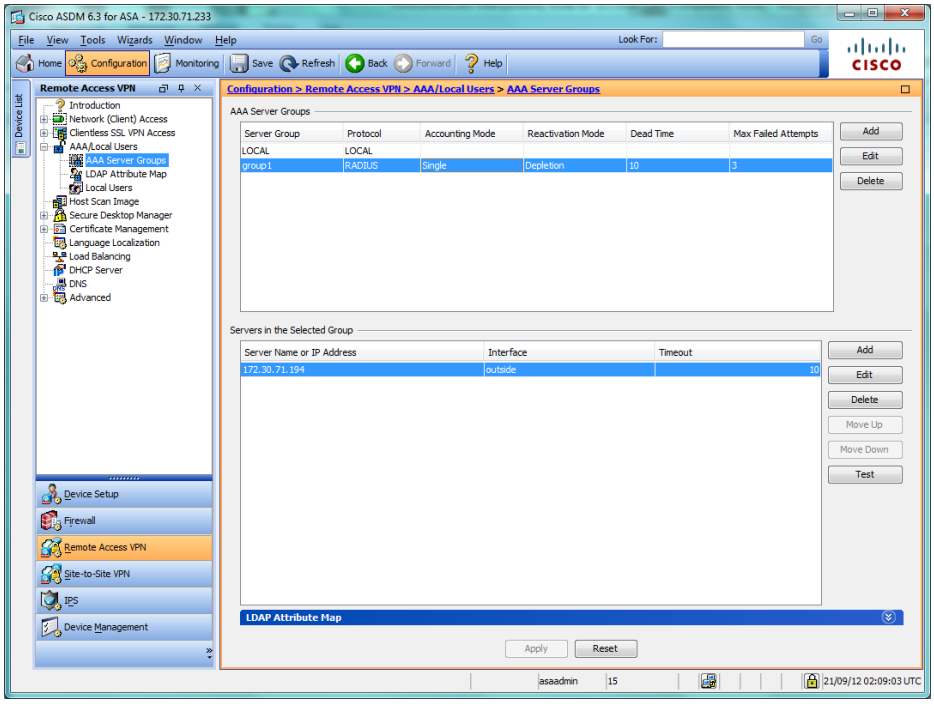
- In the Authentication tab, under Require authentication for the following types of connection, select the mode for which you wish to employ FortiAuthenticator two-factor authentication e.g. HTTP/ASDM Management as shown.



Configuring Remote Access Authentication

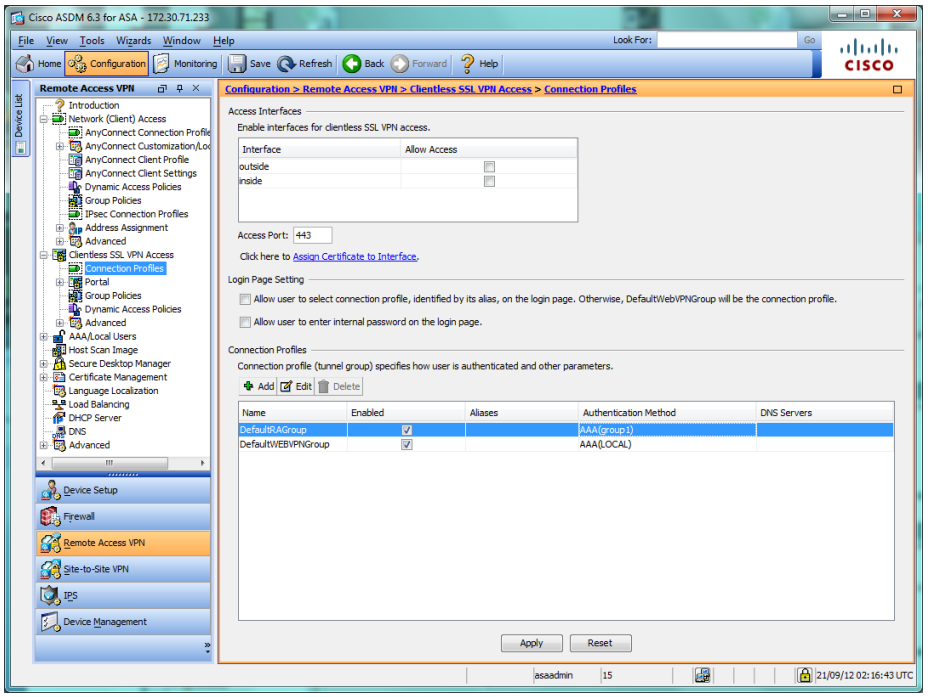
To configure authentication for Remote Access VPN, the configuration from the previous step is repeated.

- In Remote Access VPN → AAA/Local Users → AAA Server Groups, Select Add and create a group
- Create a server and add the server to the group



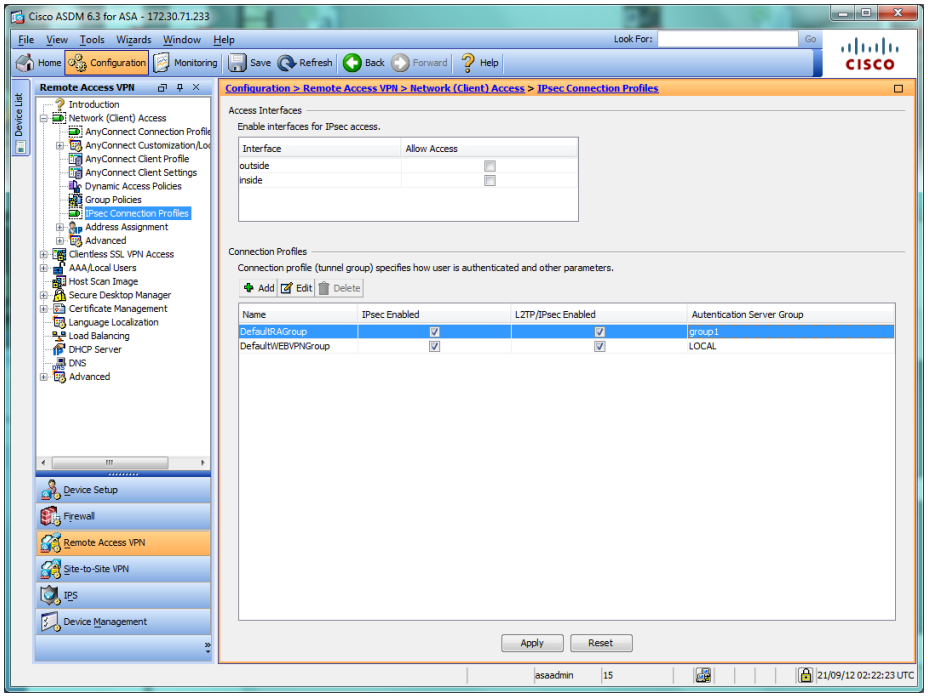
To enable two-factor authentication with FortiAuthenticator on the SSL-VPN

- Browse to Remote Access-VPN → Clientless SSL VPN Access → Connection Profiles and set the required group members to the Authentication Method (RADIUS) and Group created in the previous step



To enable two-factor authentication with FortiAuthenticator on the IPSEC VPN

- Browse to Remote Access-VPN → Network (Client) Access → IPSEC Connection Profiles and set the required group members to the Authentication Method (RADIUS) and Group created in the previous step

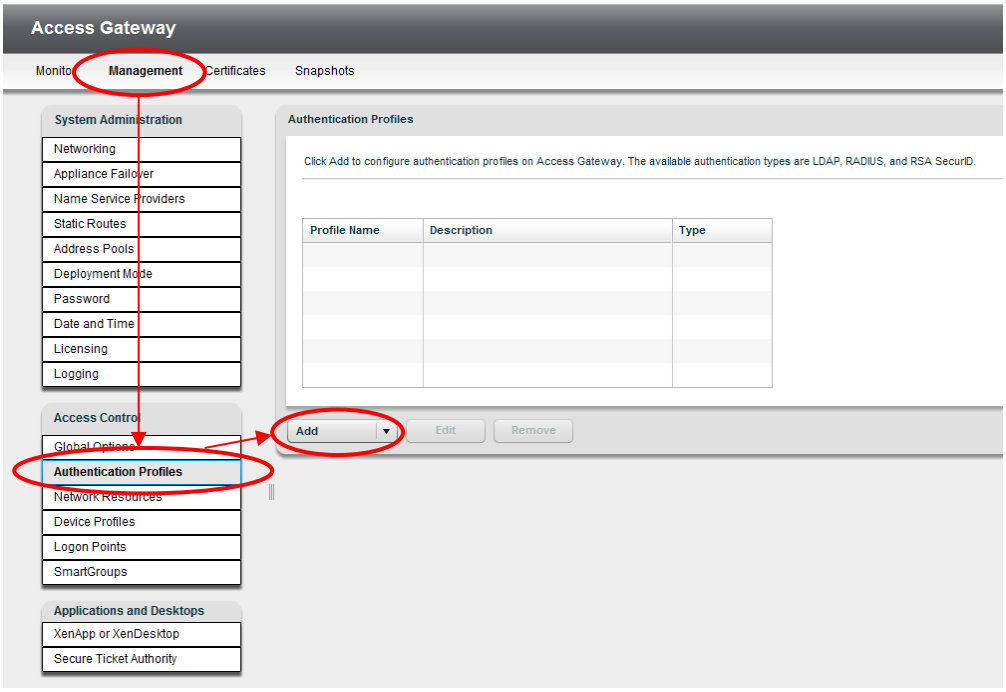

Cisco ASDM 6.3 for ASA - 172.30.71.233
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow Access
outside
inside
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Autentication Server Group
DefaultRAGroup
group1
DefaultWEBVPNGroup
LOCAL
Apply
Reset
asaadmin
15
21/09/12 02:22:23 UTC

Citrix Access Gateway

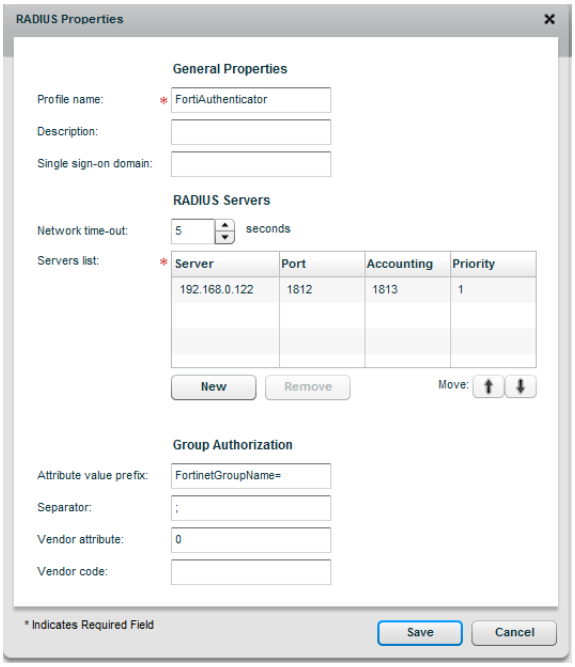
Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the Citrix Access Gateway Management GUI https://<Management_IP/lp/adminlogonpoint and browse to Management Access → Control → *Authentication Profiles*. Select ***Add***.



Enter the details of the remote FortiAuthenticator including the IP Address and shared secret and click ***Save***



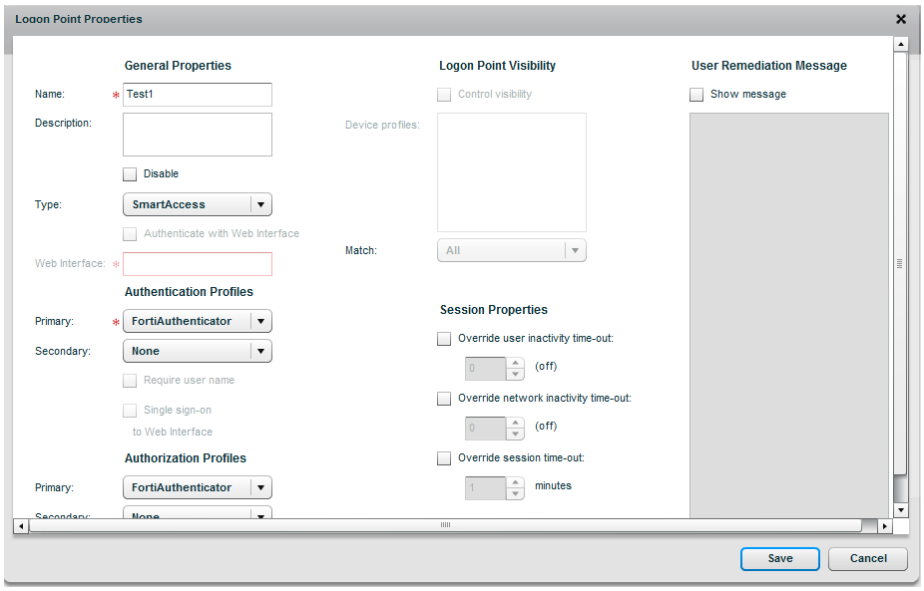
Create a logon point

Note:

A logon point in Citrix Access Gateway is the URL to which the user logs on to access a protected resource. In this example, a test Logon Point is created but the same detail can be used to modify an existing Logon Point

Browse to Access Control → *Logon Points*. Select ***New***.

Create a Test logon point e.g. ***Test1*** with *type* ***SmartAccess***. Select the FortiAuthenticator as the Primary Authentication Profile as created in the previous section. Optionally configure an authorisation profile using the same FortiAuthenticator settings. Select ***Save***.



User logon to the Citrix Access Gateway

There are 2 option for FortiAuthenticator authenticated logon to the Citrix Access Gateway:

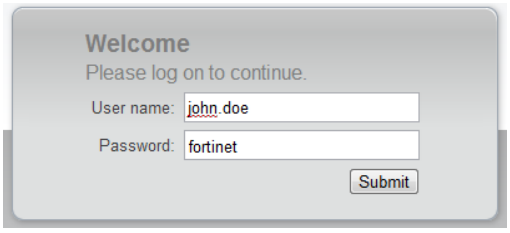
- Token Appended
- Challenge-Response

Challenge-Response is the most simple method for users and is shown below

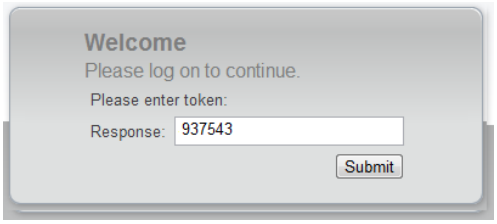
Attempt to log into the Citrix Access Gateway User GUI with the user credentials from the FortiAuthenticator. The Username and Password can be entered without the token PIN e.g.

```
Username:    john.doe
Password:    <password>
```

e.g. for a Password “fortinet” and one-time PIN of 937543, the login would become

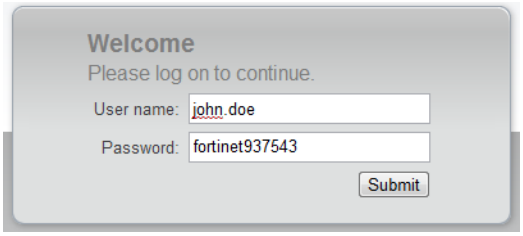


However obviously the password would be starred out. The FortiAuthenticator detects the missing token PIN and sends a RADIUS challenge which the Citrix Access Gateway presents to the user



Successful authentication will provide the user with access to the Citrix Access Gateway resource.

As an alternative a single step login can be made to bypass the challenge using the token appended method e.g.



Successful authentication will provide the user with access to the Citrix Access Gateway resource and will generate a login event in *Monitor → Audit*

```
192.168.0.254 - 0xb0409002a18b9b1:john.doe\:Test1: [04/Apr/2012:06:08:41 -0700] ""
- - "" "" Login "NavUI"
```

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong.

F5 Big-IP

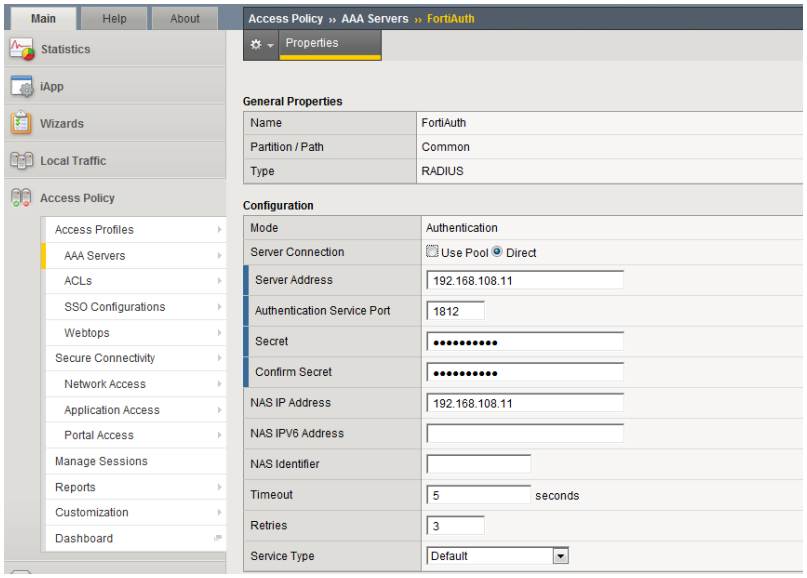
Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The following configuration was performed on an F5 Big-IP Edge Gateway device however, given the shared OS, this configuration should also be transferrable to other devices in the Big-IP range including LTM (Local Traffic Manager).

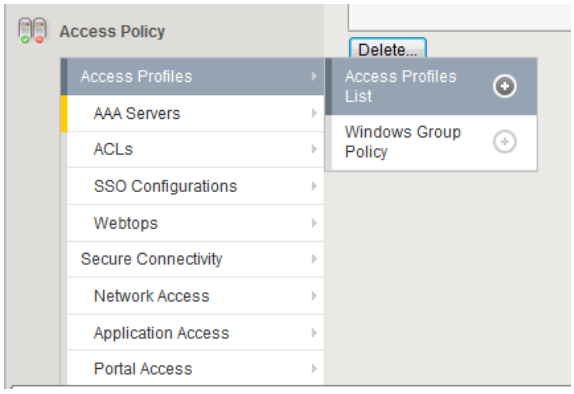
Configure the AAA Server

Log into the F5 Big-IP device and browse to *Main → Access Policy → AAA Servers → RADIUS* and select the **+** symbol to add a new configuration

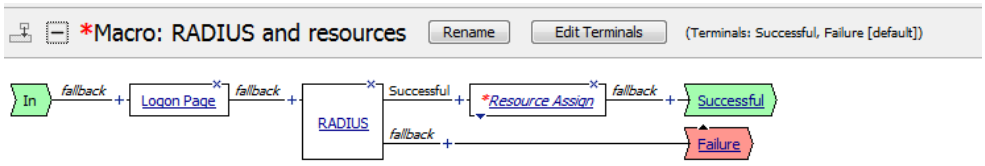
Enter the details of the FortiAuthenticator including IP (Server) Address, port and Secret.



Next browse to Main → Access Policy → Access Profiles → Access Profiles List and select the + symbol to add a new configuration

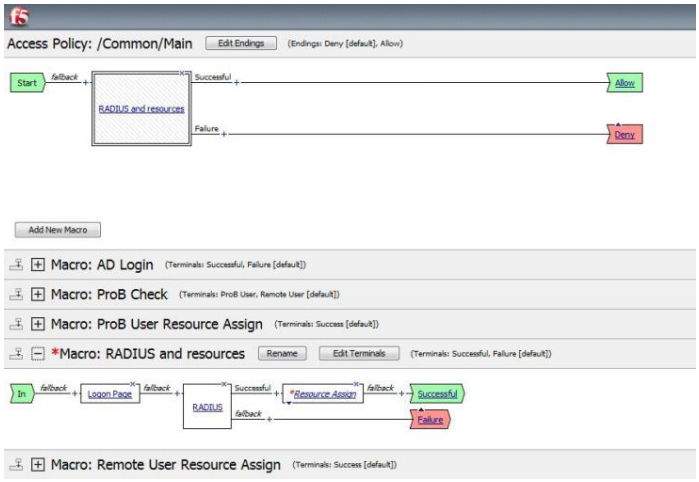


Create a RADIUS resource profile. See the F5 documentation for detailed explaination of this section however, in summary, this binds the RADIUS authentication method to the to the Logon Page defines what happens on successful or unsuccessful authentication.

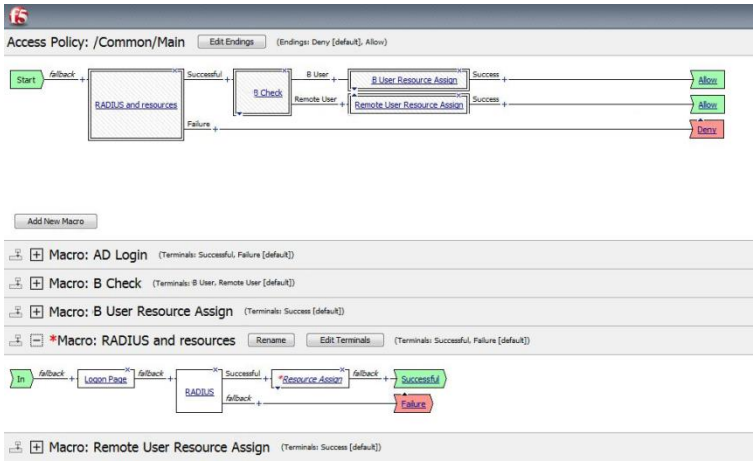


Edit the RADIUS object and define the correct details for the FortiAuthenticator as created in the previous Access Policy step (Server defined as FortiAuth). Note that extended errors may be useful for debugging but should be disabled during normal operation.

Once the RADIUS Authentication method has been defined, it should be configured for use in the Main Access Policy.



Additional validation steps can be defined if required.



Subsequent attempts to authenticate with token enabled users will result in an additional challenge prompting for the token.

User logon to the F5 Big-IP Management interface

There are 2 option for FortiAuthenticator authenticated logon to the F5 Big-IP device:

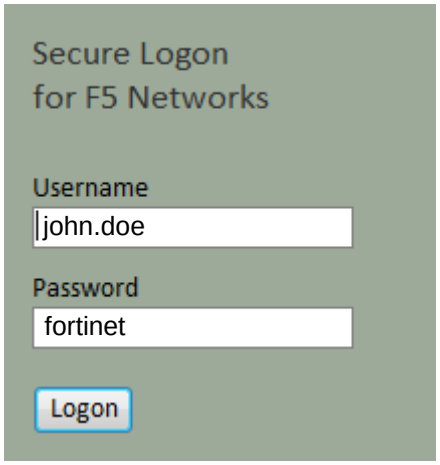
- Token Appended
- Challenge-Response

Challenge-Response is the most simple method for users and is shown below.

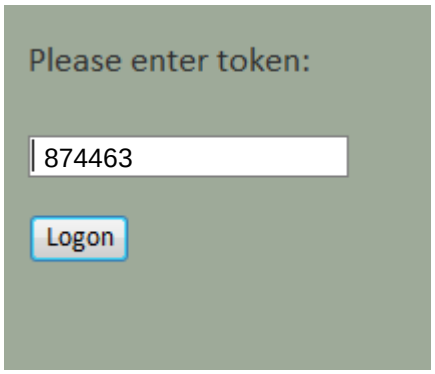
Attempt to log into the F5 Big-IP User GUI with the user credentials from the FortiAuthenticator. The Username and Password can be entered without the token PIN e.g.

```
Username:    john.doe
Password:    <password>
```

e.g. for a Password “fortinet” and one-time PIN of 874463, the login would become

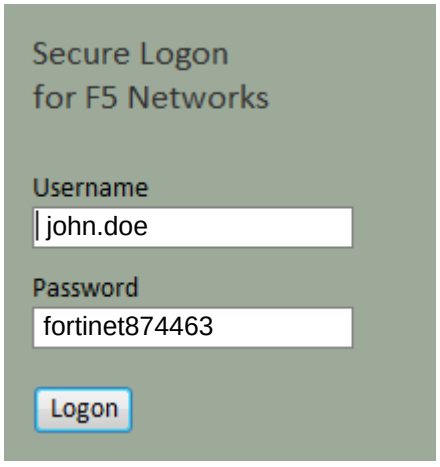


However obviously the password would be starred out. The FortiAuthenticator detects the missing token PIN and sends a RADIUS challenge which the F5 Big-IP presents to the user



Successful authentication will provide the user with access to the F5 Big-IP resource.

As an alternative a single step login can be made to bypass the challenge using the token appended method e.g.



If authentication is unsuccessful, follow the steps in the Appendix A – Debugging to identify what is wrong.

Linux Login

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Linux uses Pluggable Authentication Modules (PAM) to extend the usual local authentication methods out to external third party devices.

This makes Linux is very flexible in how it can be integrated with two-factor authentication. Applications can be configured so that e.g. locally accessed services can be authenticated via password only whilst applications accessible over the internet can be authenticated using strong two-factor methods.

The instructions below are for Ubuntu 11.04 however, PAM is pretty standard across all Linux distributions so the instructions should be usable with only minor changes.

Integrating Linux with RADIUS (FortiAuthenticator)

In order to integrate with RADIUS authentication and therefore FortiAuthenticator, first you must install the PAM RADIUS Module

```
$ sudo apt-get install libpam-radius-auth
```

Once installed, edit */etc/pam_radius_auth.conf*. The default configuration will contain the following examples (commented out):

```
#127.0.0.1      secret            1
#other-server    other-secret       3
```

To configure the FortiAuthenticator, add an additional line of the format

```
<FortiAuthenticator Name / IP>   <RADIUS Shared secret>   <Timeout>
```

e.g.

```
192.168.0.110       fortinet    3
```

To configure the FortiAuthenticator, add an additional line of the format

Enabling Strong Authentication for SSH

Caution.

Before configuring, make sure that the user you are trying to authenticate already exists on the Linux system. This limitation will be covered in a later section.

To enable two factor authentication in SSH by editing the file */etc/pam.d/ssh* and insert the following lines in before the line `# Standard Un*x authentication`

```
# Enable Two-Factor Authentication with FortiAuthenticator
auth       sufficient     pam_radius_auth.so         debug
```

Note:
The debug option at the end of the line increases debugging sent to /var/log/auth.log and can be removed once successfully configured.

Attempt to log into SSH using your chosen client with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username:     john.doe
Password:     <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 947826, the login would become

```
login as: john.doe
Password: fortinet947826
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-10-generic i686)
Last login: Mon Aug 22 18:09:18 2011 from 192.168.0.24
john.doe@Scooter:~$
```

However obviously the password would be starred out.

Successful authentication will provide the user with access to the system via SSH and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in Appendix A – Debugging to identify what is wrong.

Enabling Challenge-Response

The configuration described above requires the user to log in with the RADIUS username and password appended with the PIN. The benefit of this is that it supports almost any system which can authenticate with RADIUS. However, the FortiAuthenticator also supports a challenge-response mechanism. When the platform detects that only the password has been returned, it will respond with a RADIUS Challenge-Response and expect the PIN to be returned. This requires the client to support this additional step which the OpenSSH server does.

To configure this step on the SSH Server, edit */etc/ssh/sshd_config* and change

```
ChallengeResponseAuthentication no
```

to

```
ChallengeResponseAuthentication yes
```

And restart the SSH Server to apply the setting

```
$ sudo restart ssh
```

Apache Web Server

Caution: Before proceeding, ensure that you have followed the steps detailed in Chapter titled “Basic Configuration”. Pay particularly attention to Configure a RADIUS Client and ensure you have created a RADIUS Client entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

This document details how to enable RADIUS authentication in Apache2 for use with FortiAuthenticator two-factor authentication. If Apache2 is not installed, install it with

```
sudo apt-get install apache2
```

The Ubuntu 11.04 build of Apache2 comes with the mod-auth-radius module installed and enabled, however, if you need to manually install it

```
sudo apt-get install libapache2-mod-auth-radius
```

and enable it with

```
a2enmod auth_radius
```

At this point, confirm that you can browse to the Apache2 server via http://localhost/ or via the IP/FQDN of your test server.

Modifying the Apache configuration

There is a great deal of documentation on the internet recommending where to place the relevant configurations lines about to be described. The majority of this does not appear to work with the current installation of Apache2 on Ubuntu 11.04 for whatever reason.

The majority of documentation recommends that the RADIUS server configuration is put into */etc/apache2/apache2.conf* or */etc/apache2/httpd.conf* however, this does not work and generates an error in the */var/log/apache2/error.log*

```
[warn] AuthRadiusActive set, but no RADIUS server IP - missing AddRadiusAuth in this
context?
```

The following has been tested and confirmed to work correctly.

Edit the default site */etc/apache2/sites-enabled/000-default* , or your specific server site if this is configured, adding the lines shown in **red** in the positions specified:

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        AddRadiusAuth 192.168.0.110:1812 fortinet 5:3
        AddRadiusCookieValid 5
        DocumentRoot /var/www
        <Directory />
                Options FollowSymLinks
                AllowOverride None
                AuthType Basic
                AuthName "FortiAuthenticator Secure Authentication"
                AuthBasicAuthoritative Off
                AuthBasicProvider radius
                AuthRadiusAuthoritative on
                AuthRadiusActive On
                Require valid-user
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
```

```
</Directory>
```

When completed, restart the Apache2 daemon

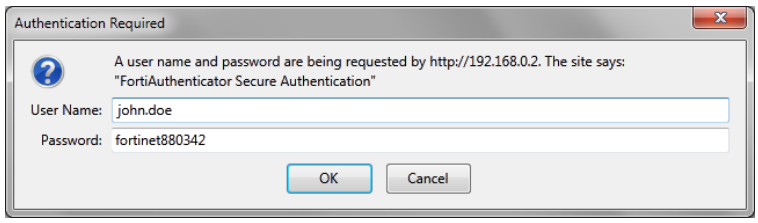
```
sudo /etc/init.d/apache2 restart
```

Clear the cache on your browser and restart to avoid any locally cached content from being displayed without the need for authentication (can be confusing when debugging).

Browse to the web site configured e.g. http://localhost/ and you should be prompted for your credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

```
Username:    john.doe
Password:    <password><Token PIN>
```

e.g. for a Password “fortinet” and one-time PIN of 880342, the login would become



However obviously the password would be starred out.

Successful authentication will provide the user with access to the page and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter *Debugging Authentication* to identify what is wrong. Additional debugging can be performed using the Apache2 logs located in */var/log/apache2*. Most useful is the error.log which will display a log if the RADIUS server credentials are incorrectly configured.

Appendix A – Debugging

FortiAuthenticator is incredibly simple to get working however, should you encounter difficulty there are some simple steps which can be taken to diagnose the problem.

Logging

If authentication is failing on your RADIUS CLIENT , the first place to check to see why is the FortiAuthenticator log files.

Bad Password

Pretty self-explanatory, try resetting the password if the user insists they have the correct credentials.

If this persists, verify that the pre-shared secret is correct on both the RADIUS Client and the FortiAuthenticator.

Bad Token Code

This may be due to user error (entering the incorrect Token) or may be caused by time issues.

To debug this issue, verify the following:

- Ensure the user is not trying to use a previously used Token number. i.e. you cannot log in twice with the same Token number.
- The time and time zone on the FortiAuthenticator is correct and preferably synchronised using NTP.
- The Token is correctly synced with the FortiAuthenticator. Verify the drift by syncing the token as shown in Section

Nothing Logged

If there is no failure or successful authentication logged. This will be generally be due to one of two things:

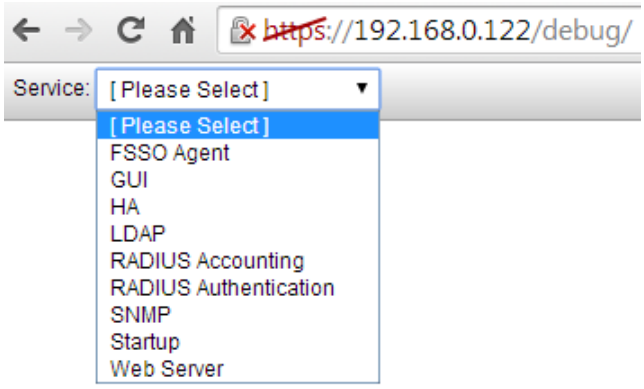
- **Request is not reaching the FortiAuthenticator.** Verify that any intervening firewalls are permitting the required traffic through the network. RADIUS Authentication traffic will require UDP Port 1812 opening to the FortiAuthenticator and pseudo-stateful responses allowed to return.
- **Request is reaching the FortiAuthenticator but is being ignored.** If traffic is seen reaching the FAC (e.g. by packet sniffing) but is being ignored, it is most likely that the requesting RADIUS Client not configured in the FortiAuthenticator. Verify that the RADIUS Client is sending the traffic from the expected IP and not from a secondary IP or alternative interface. The FortiAuthenticator RADIUS server will not respond to requests from an unknown RADIUS Client for security reasons.

One other, less likely possibility is the NAS_Calling_IP Attribute is set to an incorrect value.

Extended Logging

The standard GUI Logs found Logging → Log Access → Logs provide a concise summary of events occurring on the system, particularly the information needed for audit purposes (who logged in, when and where from). However there are times when a more detailed view is required in order to debug issues.

Detailed syste and application logs can be found by browsing to https://<FAC_IP>/debug/

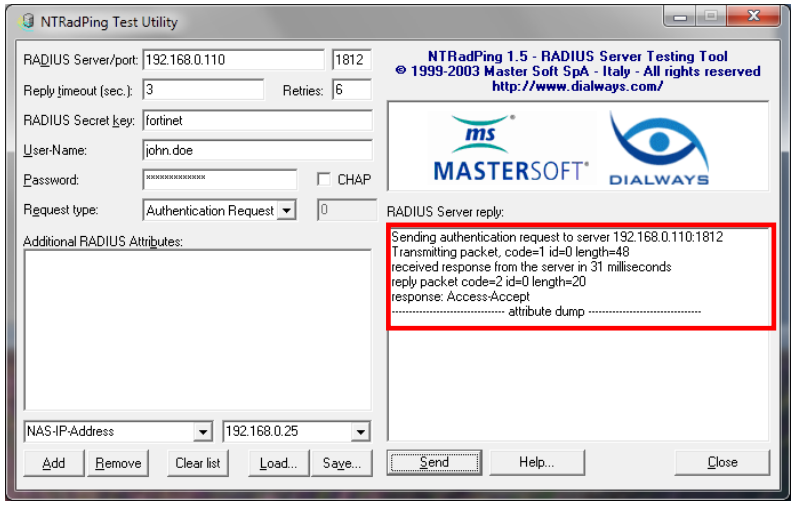


There are several log files as detailed below with the most useful **highlighted in Bold**:

FSSO Agent	Details of Fortinet Single Sign-On events
GUI	Errors encountered whilst rendering the appliance GUI
HA	**Details of and errors in the HA process**
LDAP	**Details of the LDAP authentication process for both local and remote connections**
RADIUS Accounting	Details of the RADIUS Accounting Proxy engine
RADIUS Authentication	**Details of the RADIUS authentication process**
SNMP	Details of the SNMP Daemon
Startup	Errors during creation of the initial database and during the system startup
Web Server	Errors encountered by the WebServer

RADIUS Packet Generation

Testing authentication directly without the use of a NAS device is useful to rule out issues with the NAS device. This is most easily achieved by using a tool such as NTRADPing


NTRadPing Test Utility
RADIUS Server/port: 192.168.0.110 1812
Reply timeout (sec.): 3 Retries: 6
RADIUS Secret key: fortinet
User-Name: john.doe
Password: ********** CHAP
Request type: Authentication Request 0
Additional RADIUS Attributes:
NAS-IP-Address 192.168.0.25
Add Remove Clear list Load... Save...
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
MASTERSOFT
DIALWAYS
RADIUS Server reply:
Sending authentication request to server 192.168.0.110:1812
Transmitting packet, code=1 id=0 length=48
received response from the server in 31 milliseconds
reply packet code=2 id=0 length=20
response: Access-Accept
---------- attribute dump ----------
Send Help... Close

Appendix B – Supported Two-Factor Authentication Methods

FortiOS

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users	Access Override	Tested Version
FortiGate 5.0	**NAT Route Mode**						
	Web Based Management	Supported	Supported	Supported	Supported	Supported	**FortiGate 5.0 PR7**
	SSH Based Management	Supported	Supported	Supported	Supported	Supported	**FortiClient 5.0.9**
	Telnet Management	Supported	Supported	Supported	Supported	Supported	
	IPSEC VPN (FortiClient)	Supported	Supported	Supported	Supported	Supported	
	SSL VPN (Web)	Supported	Supported	Supported	Supported	Supported	
	SSL VPN (FortiClient)	Supported	Supported	Supported	Supported	Supported	
	Identity Based Policy	Supported	Supported	Supported	Supported		
	Web Filtering Overrride	Not Supported	Supported	Not Supported	Supported		
	Explicit Proxy						
	Identity Based Policy (Basic Auth)	Not Supported	Supported	Not Supported	Not Supported	Supported	
	Identity Based Policy (Forms Auth)	Not Supported	Supported	Not Supported	Not Supported	Supported	
	Web Filtering Overrride	Not Supported	Supported	Not Supported	Not Supported	Supported	
FortiGate 5.2	**NAT Route Mode**						
	Web Based Management	Supported	Supported	Supported	Supported		**FortiGate 5.2**
	SSH Based Management	Supported	Supported	Supported	Supported		**FortiClient 5.0.9**
	Telnet Management	Supported	Supported	Supported	Supported		
	IPSEC VPN (FortiClient)	Supported	Supported	Supported	Supported		
	SSL VPN (Web)	Supported	Supported	Supported	Supported		
	SSL VPN (FortiClient)	Supported	Supported	Supported	Supported		
	Identity Based Policy	Supported	Supported	Supported	Supported		
	Web Filtering Overrride	Not Supported	Supported	Not Supported	Supported		
	Explicit Proxy						
	Identity Based Policy (Basic Auth)	Not Supported	Supported	Not Supported	Not Supported		
	Identity Based Policy (Forms Auth)	Not Supported	Supported	Not Supported	Not Supported		
	Web Filtering Overrride	Not Supported	Supported	Not Supported	Not Supported		

Other Fortinet products

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users	Access Override	Tested Version
FortiManager 5.0	Web Based Management	Not Supported	Supported	Not Supported [1]	Supported	Supported	**FortiManager 5.0.6**
	SSH Based Management	Not Supported	Supported	Supported	Supported	Supported	
	Telnet Management	Not Supported	Supported	Supported	Supported	Supported	
FortiManager 5.2	Web Based Management	Not Supported	Supported	Supported	Supported	Supported	**FortiManager 5.2 (beta 2)**
	SSH Based Management	Not Supported	Supported	Supported	Supported	Supported	
	Telnet Management	Not Supported	Supported	Supported	Supported	Supported	
FortiAnalyzer 5.0	Web Based Management	Not Supported	Supported	Not Supported [1]	Supported	Supported	**FortiAnalyzer 5.0.6**
	SSH Based Management	Not Supported	Supported	Supported	Supported	Supported	
	Telnet Management	Not Supported	Supported	Supported	Supported	Supported	
FortiMail 5.1	Web Based Management	Not Supported	Supported	Not Supported [2]	Supported	Supported	**FortiMail 5.1.3**
	SSH Based Management	Not Supported	Supported	Not Supported [2]	Supported	Supported	
	Telnet Management	Not Supported	Supported	Not Supported [2]	Supported	Supported	
FortiWeb 5.2	Web Based Management	Not Supported	Supported	Not Supported [3]	Supported		**FortiWeb 5.2.1**
	SSH Based Management	Not Supported	Supported	Not Supported [3]	Supported		
	Telnet Management	Not Supported	Supported	Not Supported [3]	Supported		

[1] Mantis : 0245870 & 0242915 - GUI Token Challenge Page broken in FortiManager/FortiAnalyzer 5.0.6. Fixed in the forthcoming 5.0.7 and 5.2.

[2] Mantis 0245948: Token challenge not supported in FortiMail 5.0.3. Workaround: use token appended. Fix planned in next release.

[3] Mantis 0246032: Token challenge not supported in FortiWeb 5.2.1 Workaround: use token appended. Fix planned in future release.

Third Party Products

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users	Access Override	Tested Version
Citrix Access Gateway	Web Based Management	Not Supported	Supported	Supported	Supported		**Citrix Access Gateway 5.0**
	SSH Management	Not Supported	Supported	Supported	Supported		
	Web Based User Authentication	Not Supported	Supported	Supported	Supported		
Cisco ASA	Web Based Management	Not Supported	Supported	Supported	Supported		**Cisco ASA 8.2(1)**
	SSH Management	Not Supported	Supported	Supported	Supported		
	SSL-VPN	Not Supported	Supported	Supported	Supported		
	IPSEC VPN	Not Supported	Supported	Supported	Supported		
F5 BIG-IP EG	Web Based Management	Not Supported	Supported	Supported	Supported		**TMOS 11.2.1**
	SSH Management	Not Supported	Supported	Supported	Supported		
SSH	SSH Login	Not Supported	Supported	Supported	Supported		**OpenSSH version 5.8p1**
Apache	Web Authentication	Not Supported	Supported	Supported	Supported		**Apache 2.2.17**

Appendix C – Syncing FortiTokens

Under most circumstances, it is not necessary to synchronise a FortiToken unless the time on the host FortiAuthenticator system has been allowed to deviate from the correct time. It is essential that the time is kept accurate at all times to prevent issues occurring so configuration of an NTP server is recommended.

Under normal operation, the natural drift of the time on the FortiToken (as found in all clocks) is accounted for automatically by the FortiAuthenticator. Every time a user logs in, the FortiAuthenticator calculates the drift and if it is within +/- 1 (where 1 is a token cycle of 60 seconds), the drift is adjusted accordingly. Should the drift deviate by greater than 1 (i.e. the clock is more than 60 seconds out) since the last login, a manually synchronisation is required.

Note:

If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

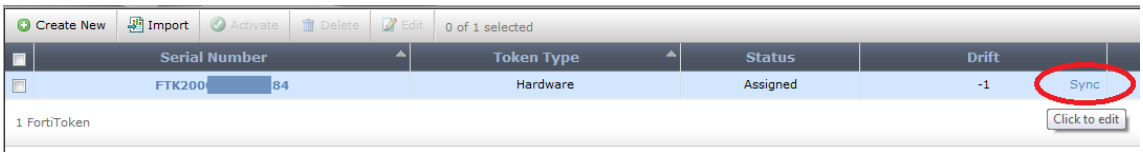
Administrator Synchronisation

It is possible for the administrator to synchronise a token for use on the FortiAuthenticator and sometime advisable when issuing new tokens which have been held in storage for an extended period or are being reissued.

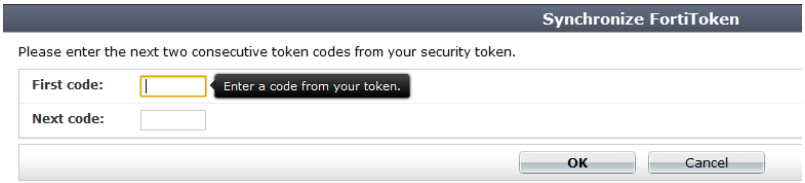
Note:

If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

Browse to *Authentication → FortiTokens* and hover the mouse over the required token drift category. An option to *sync* will appear



Select Sync and follow instructions to input 2 consecutive Token PINs.



Key points to note during the Synchronization process are:

- Ensure that the FortiAuthenticator time is accurate before proceeding
- Ensure the serial of the token you are trying to synchronize matches that on the reverse of the token.

- Ensure that the token has not been used in the preceding 60 seconds. All tokens are one time passwords and cannot therefore be used to authenticate (successful or otherwise) and synchronize.
- Once successfully synchronized, wait a further 60 seconds before attempting to log in. A token used to synchronize cannot be re-used to authenticate.

User Synchronisation

Should it be required, FortiAuthenticator provides a mechanism for the user to perform their own manual synchronization. The user should be allowed to access the FortiAuthenticator WebUI e.g https:/<FAC_IP>/login/.

On logging into the FortiAuthenticator the user will be prompted to enter their token PIN. If the token PIN is out of sync, they will be prompted to enter 2 consecutive PINs. If the user receives no such prompt, the token is already correctly synchronized.